IFS NS3552-8P-2S and NS3550-2T-8S User Manual

P/N 1072687 • REV A • ISS 19DEC13

Copyright © 2013 United Technologies Corporation

Interlogix is part of UTC Climate Controls & Security, a unit of United Technologies Corporation. All rights reserved.

Trademarks and patents The IFS NS3552-8P-2S and NS3550-2T-8S name and logo are trademarks of United Technologies.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer Interlogix

3211 Progress Drive, Lincolnton, NC 28092 USA

Authorized EU manufacturing representative:
UTC Climate Controls & Security B.V.,
Kelvinstraat 7, 6003 DH Weert, Netherlands

Intended use Use this product only for the purpose it was designed for; refer to the data sheet and user documentation for details. For the latest product information, contact your local supplier or visit us online at www.interlogix.com.

Certification CE N4131

FCC compliance This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

You are cautioned that any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

ACMA compliance **Notice!** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Canada This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme á la norme NMB-003du Canada.

European Union directives **2004/108/EC (EMC Directive):** Hereby, UTC Climate Controls & Security Corporation, Inc. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC.

Contact Information For contact information, see www.interlogix.com or www.utcfssecurityproducts.eu.

TABLE OF CONTENTS

IFS NS3552-8P-2S and NS3550-2T-8S User Manual 1

1. INTRODUCTION 24

1.1 Packet Contents 24

1.2 Product Description 25

1.3 How to Use This Manual 29

1.4 Product Features 30

1.5 Product Specifications 34

2. INSTALLATION 38

2.1 Hardware Descriptions 38

2.1.1 Physical Dimensions 38

2.1.2 Front Panel 39

2.1.3 LED Indicators 41

2.1.4 Wiring the Power Input 42

2.1.5 Wiring the Fault Alarm Contact 42

2.1.6 Wiring the Digital Input / Output 44

2.2 Install the Industrial Managed Switch 46

2.2.1 Installation Steps 46

2.2.2 DIN-Rail Mounting 47

2.2.3 Wall Mount Plate Mounting 49

2.3 Cabling 50

2.3.1 Installing the SFP Transceiver 51

2.3.2 Remove the Module 53

3. SWITCH MANAGEMENT 54

3.1 Requirements 54

3.2 Management Access Overview 55

3.3 CLI Mode Management 56

3.4 Web Management 58

3.5 SNMP-Based Network Management 59

4. WEB CONFIGURATION 60

4.1 Main Web Page 63

4.2 System 65

4.2.1 System Information 65
4.2.2 IP Configuration 66
4.2.3 IPv6 Configuration 68
4.2.4 Users Configuration 69
4.2.5 Privilege Levels 71
4.2.6 NTP Configuration 73
4.2.7 Daylight Saving 74
4.2.8 UPnP 76
4.2.9 DHCP Relay 78
4.2.10 DHCP Relay Statistics 79
4.2.11 CPU Load 80
4.2.12 System Log 81
4.2.13 Detailed Log 83
4.2.14 Remote Syslog 83
4.2.15 SMTP Configuration 85
4.2.16 Digital Input/output 86
4.2.17 Fault Alarm 88
4.2.18 EEE Power Reduction 89
4.2.19 Web Firmware Upgrade 90
4.2.20 TFTP Firmware Upgrade 91
4.2.21 Configuration Backup 92
4.2.22 Configuration Upload 93
4.2.23 Image Select 95
4.2.24 Factory Default 96
4.2.25 System Reboot 97

4.3 Simple Network Management Protocol 98

4.3.1 SNMP Overview 98
4.3.2 SNMP System Configuration 99
4.3.3 SNMP System Information 101
4.3.4 SNMPv3 Configuration 102
4.3.4.1 SNMPv3 Communities 102
4.3.4.2 SNMPv3 Users 103
4.3.4.3 SNMPv3 Groups 104
4.3.4.4 SNMPv3 Views 105
4.3.4.5 SNMPv3 Access 105

4.4 Port Management 107

4.4.1 Port Configuration 107
4.4.2 Port Statistics Overview 109
4.4.3 Port Statistics Detail 110
4.4.4 SFP Information 111
4.4.5 Port Mirror 113

4.5 Link Aggregation 115
4.5.1 Static Aggregation 118
4.5.2 LACP Configuration 120
4.5.3 LACP System Status 121
4.5.4 LACP Port Status 122
4.5.5 LACP Port Statistics 122

4.6 VLAN 124
4.6.1 VLAN Overview 124
4.6.2 IEEE 802.1Q VLAN 124
4.6.3 VLAN Basic Information 128
4.6.4 VLAN Port Configuration 128
4.6.5 VLAN Membership 133
4.6.6 VLAN Membership Status 134
4.6.7 VLAN Port Status 136
4.6.8 Private VLAN 137
4.6.9 Port Isolation 138
4.6.10 VLAN Setting Example: 139
4.6.10.1 Two separate 802.1Q VLAN 140
4.6.10.2 VLAN Trunking between two 802.1Q aware Switch 143
4.6.10.3 Port Isolate 145
4.6.11 MAC-based VLAN 146
4.6.12 MAC-based VLAN Status 147
4.6.13 Protocol-based VLAN 148
4.6.14 Protocol-based VLAN Membership 149

4.7 Spanning Tree Protocol 151
4.7.1 Theory 151
4.7.2 STP System Configuration 157
4.7.3 Bridge Status 159
4.7.4 CIST Port Configuration 160
4.7.5 MSTI Priorities 163
4.7.6 MSTI Configuration 164
4.7.7 MSTI Ports Configuration 165
4.7.8 Port Status 167
4.7.9 Port Statistics 168

4.8 Multicast 170
4.8.1 IGMP Snooping 170
4.8.2 IGMP Snooping Configuration 174
4.8.3 IGMP Snooping VLAN Configuration 175
4.8.4 IGMP Snooping Port Group Filtering 176
4.8.5 IGMP Snooping Status 179
4.8.6 IGMP Group Information 180
4.8.7 IGMPv3 Information 181
4.8.8 MLD Snooping Configuration 181
4.8.9 MLD Snooping VLAN Configuration 183
4.8.10 MLD Snooping Port Group Filtering 185
4.8.11 MLD Snooping Status 186
4.8.12 MLD Groups Information 187
4.8.13 MLDv2 Information 188
4.8.14 MVR 189
4.8.15 MVR Status 191
4.8.16 MVR Groups Information 191
4.8.17 MVR SFM Information 192

4.9 Quality of Service 194
4.9.1 Understand QOS 194
4.9.2 Port Policing 195
4.9.3 Port Shaping 195
4.9.3.1 QoS Egress Port Schedule and Shapers 196
4.9.4 Port Classification 198
4.9.4.1 QoS Ingress Port Tag Classification 199
4.9.5 Port Scheduler 200
4.9.6 Port Tag Remarking 201
4.9.6.1 QoS Egress Port Tag Remarking 201
4.9.7 Port DSCP 202
4.9.8 DSCP-Based QoS 204
4.9.9 DSCP Translation 205
4.9.10 DSCP Classification 207
4.9.11 QoS Control List 208
4.9.11.1 QoS Control Entry Configuration 209
4.9.12 QoS Status 210
4.9.13 Queue Policing 211
4.9.14 Storm Control Configuration 212
4.9.15 QoS Statistics 213
4.9.16 Voice VLAN Configuration 215
4.9.17 Voice VLAN OUI Table 217

4.10 Access Control Lists 217
4.10.1 Access Control List Status 218
4.10.2 Access Control List Configuration 220
4.10.3 ACE Configuration 222
4.10.4 ACL Ports Configuration 228
4.10.5 ACL Rate Limiter Configuration 230

4.11 Authentication 232
4.11.1 Understanding IEEE 802.1X Port-Based Authentication 233
4.11.2 Authentication Configuration 237
4.11.3 Network Access Server Configuration 238
4.11.4 Network Access Overview 244
4.11.5 Network Access Statistics 245
4.11.6 Authentication Server Configuration 251
4.11.7 RADIUS Overview 253
4.11.8 RADIUS Details 256
4.11.9 Windows Platform RADIUS Server Configuration 260
4.11.10 802.1X Client Configuration 265

4.12 Security 268
4.12.1 Port Limit Control 268
4.12.2 Access Management 272
4.12.3 Access Management Statistics 272
4.12.4 HTTPs 274
4.12.5 SSH 275
4.12.6 Port Security Status 275
4.12.7 Port Security Detail 278
4.12.8 DHCP Snooping 278
4.12.9 DHCP Snooping Statistics 280
4.12.10 IP Source Guard Configuration 282
4.12.11 IP Source Guard Static Table 283
4.12.12 ARP Inspection 284
4.12.13 ARP Inspection Static Table 285

4.13 MAC Address Table 286
4.13.1 MAC Address Table Configuration 286
4.13.2 MAC Address Table Status 288
4.13.3 Dynamic ARP Inspection Table 289
4.13.4 Dynamic IP Source Guard Table 290

4.14 LLDP 292
4.14.1 Link Layer Discovery Protocol 292
4.14.2 LLDP Configuration 292

4.14.3 LLDP-MED Configuration 294
4.14.4 LLDP-MED Neighbor 301
4.14.5 Neighbor 304
4.14.6 Port Statistics 304

4.15 Diagnostics 307
4.15.1 Ping 308
4.15.2 IPv6 Ping 309
4.15.3 Remote IP Ping Test 309
4.15.4 Cable Diagnostics 311

4.16 Power over Ethernet 312
4.16.1 Power over Ethernet Powered Device 313
4.16.2 System Configuration 314
4.16.3 Port Configuration 317
4.16.4 PoE Status 318
4.16.5 PoE Schedule 320
4.16.6 LLDP PoE Neighbors 323
4.16.7 PoE Alive Check Configuration 324

4.17 Loop Protection 326
4.17.1 Configuration 326
4.17.2 Status 327

4.18 RMON 329
4.18.1 RMON Alarm Configuration 329
4.18.2 RMON Alarm Status 331
4.18.3 RMON Event Configuration 332
4.18.4 RMON Event Status 333
4.18.5 RMON History Configuration 333
4.18.6 RMON History Status 334
4.18.7 RMON Statistics Configuration 335
4.18.8 RMON Statistics Status 336

4.19 Ring 338
4.19.1 MEP Configuration 340
4.19.2 Detailed MEP Configuration 341
4.19.3 Ethernet Ring Protocol Switch 344
4.19.4 Ethernet Ring Protocol Switch Configuration 345
4.19.5 Ring Wizard 347
4.19.6 Ring Wizard Example: 349

5. COMMAND LINE INTERFACE 352

5.1 Accessing the CLI 352

5.2 Telnet Login 352

6. COMMAND LINE MODE 353

6.1 System Command 354

System Configuration 354
System Log Configuration 354
System Timezone Configuration 355
System Version 355
System Log Server Mode 355
System Name 356
System Timezone Offset 356
System Contact 357
System Log Server Address 357
System Timezone Acronym 358
System DST Configuration 358
System Location 358
System Log Level 359
System DST Mode 359
System DST Start 360
System Log Lookup 360
System DST End 360
System Log Clear 361
System Reboot 361
System DST Offset 362
System Restore Default 362
System Load 362

6.2 IP Command 363

IP Configuration 363
IP DHCP 364
IP Setup 364
IP Ping 365
IP DNS 366
IP DNS Proxy 366
IPv6 AUTOCINFIG 367
IPv6 Setup 367
IPv6 State 368
IPv6 Ping6 368
IP NTP Configuration 369

IP NTP Mode 369
IP NTP Server Add 370
IP NTP Server IPv6 Add 370
IP NTP Server Delete 371

6.3 Port Management Command 372
Port Configuration 372
Port Mode 372
Port Flow Control 373
Port State 373
Port Maximum Frame 374
Port Power 374
Port Excessive 375
Port Statistics 376
Port VeriPHY 376
Port SFP 376
Port Description 377

6.4 MAC Address Table Command 378
MAC Configuration 378
MAC Add 378
MAC Delete 379
MAC Lookup 379
MAC Age Time 380
MAC Learning 380
MAC Dump 381
MAC Statistics 382
MAC Flush 382

6.5 VLAN Configuration Command 383
VLAN Configuration 383
VLAV PVID 384
VLAN Frame Type 384
VLAN Ingress Filter 385
VLAN Mode 385
VLAN Link Type 386
VLAN Q-in-Q Mode 386
VLAN Ethernet Type 387
VLAN untagVID 387
VLAN Add 388
VLAN Forbidden Add 388
VLAN Delete 389

VLAN Forbidden Delete....389
VLAN Forbidden Lookup....390
VLAN Lookup....390
VLAN Name Add....391
VLAN Name Delete....391
VLAN Name Lookup....392
VLAN Status....392

6.6 Private VLAN Configuration Command....393
PVLAN Configuration....393
PVLAN Add....394
PVLAN Delete....394
PVLAN Lookup....395
PVLAN Isolate....395

6.7 Security Command....396
Security Switch User Configuration....396
Security Switch User Add....396
Security Switch User Delete....397
Security Switch Privilege Level Configuration....397
Security Switch Privilege Level Group....398
Security Switch Privilege Level Current....398
Security Switch Auth Configuration....398
Security Switch Auth Method....399
Security Switch SSH Configuration....400
Security Switch SSH Mode....400
Security Switch HTTPs Configuration....401
Security Switch HTTPs Mode....401
Security Switch HTTPs Redirect....401
Security Switch Access Configuration....402
Security Switch Access Mode....402
Security Switch Access Add....403
Security Switch Access IPv6 Add....403
Security Switch Access Delete....404
Security Switch Access Lookup....405
Security Switch Access Clear....405
Security Switch Access Statistics....405
Security Switch SNMP Configuration....406
Security Switch SNMP Mode....406
Security Switch SNMP Version....407
Security Switch SNMP Read Community....407
Security Switch SNMP Write Community....408

Security Switch SNMP Trap Mode....408
Security Switch SNMP Trap Version....409
Security Switch SNMP Trap Community....409
Security Switch SNMP Trap Destination....410
Security Switch SNMP Trap IPv6 Destination....410
Security Switch SNMP Trap Authentication Failure....411
Security Switch SNMP Trap Link-up....411
Security Switch SNMP Trap Inform Mode....412
Security Switch SNMP Trap Inform Timeout....412
Security Switch SNMP Trap Inform Retry Times....413
Security Switch SNMP Trap Probe Security Engine ID....413
Security Switch SNMP Trap Security Engine ID....414
Security Switch SNMP Trap Security Name....414
Security Switch SNMP Engine ID....415
Security Switch SNMP Community Add....415
Security Switch SNMP Community Delete....416
Security Switch SNMP Community Lookup....416
Security Switch SNMP User Add....416
Security Switch SNMP User Delete....417
Security Switch SNMP User Changekey....418
Security Switch SNMP User Lookup....418
Security Switch SNMP Group Add....419
Security Switch SNMP Group Delete....419
Security Switch SNMP Group Lookup....420
Security Switch SNMP View Add....420
Security Switch SNMP View Delete....421
Security Switch SNMP View Lookup....421
Security Switch SNMP Access Add....422
Security Switch SNMP Access Delete....422
Security Switch SNMP Access Lookup....423
Security Switch RMON Statistics Add....423
Security Switch RMON Statistics Delete....424
Security Switch RMON Statistics Lookup....424
Security Switch RMON History Add....424
Security Switch RMON History Delete....425
Security Switch RMON History Lookup....425
Security Switch RMON Alarm Add....425
Security Switch RMON Alarm Delete....426
Security Switch RMON Alarm Lookup....427
Security Switch RMON Event Add....427
Security Switch RMON Event Delete....427

Security Switch RMON Event Lookup 428
Security Network Psec Switch 428
Security Network Psec Port 429
Security Network Limit Configuration 429
Security Network Limit Mode 430
Security Network Limit Aging 430
Security Network Limit Agetime 431
Security Network Limit Port 431
Security Network Limit Limit 432
Security Network Limit Action 432
Security Network Limit Reopen 433
Security Network NAS Configuration 433
Security Network NAS Mode 434
Security Network NAS State 435
Security Network NAS Reauthentication 435
Security Network NAS ReauthPeriod 436
Security Network NAS EapolTimeout 436
Security Network NAS Agetime 437
Security Network NAS Holdtime 437
Security Network NAS RADIUS_QoS 438
Security Network NAS RADIUS_VLAN 439
Security Network NAS Guest_VLAN 439
Security Network NAS Authenticate 440
Security Network NAS Statistics 441
Security Network ACL Configuration 441
Security Network ACL Action 442
Security Network ACL Policy 442
Security Network ACL Rate 443
Security Network ACL Add 443
Security Network ACL Delete 445
Security Network ACL Lookup 445
Security Network ACL Clear 445
Security Network ACL Status 446
Security Network DHCP Relay Configuration 446
Security Network DHCP Relay Mode 447
Security Network DHCP Relay Server 447
Security Network DHCP Relay Information Mode 448
Security Network DHCP Relay Information Policy 449
Security Network DHCP Relay Statistics 449
Security Network DHCP Snooping Configuration 450
Security Network DHCP Snooping Mode 450

Security Network DHCP Snooping Port Mode....450
Security Network DHCP Snooping Statistics....451
Security Network IP Source Guard Configuration....452
Security Network IP Source Guard Mode....452
Security Network IP Source Guard Port Mode....452
Security Network IP Source Guard Limit....453
Security Network IP Source Guard Entry....453
Security Network IP Source Guard Status....454
Security Network IP Source Guard Translation....454
Security Network ARP Inspection Configuration....455
Security Network ARP Inspection Mode....455
Security Network ARP Inspection Port Mode....455
Security Network ARP Inspection Entry....456
Security Network ARP Inspection Status....457
Security Network ARP Inspection Translation....457
Security AAA Configuration....457
Security AAA Timeout....458
Security AAA Deadtime....459
Security AAA RADIUS....459
Security AAA ACCT_RADIUS....460
Security AAA TACACS+....460
Security AAA Statistics....461

6.8 Spanning Tree Protocol Command....462

STP Configuration....462
STP Version....463
STP Tx Hold....463
STP MaxHops....464
STP MaxAge....464
STP FwdDelay....465
STP CName....465
STP BPDU Filter....466
STP BPDU Guard....466
STP Recovery....467
STP Status....467
STP MSTI Priority....468
STP MSTI Map....468
STP MSTI Add....469
STP Port Configuration....469
STP Port Mode....470
STP Port Edge....470

STP Port AutoEdge 471
STP Port P2P 471
STP Port RestrictedRole 472
STP Port RestrictedTcn 472
STP Port bpduGuard 473
STP Port Statistic 473
STP Port Mcheck 474
STP MSTI Port Configuration 474
STP MSTI Port Cost 475
STP MSTI Port Priority 475

6.9 Link Aggregation Command 477
Aggregation Configuration 477
Aggregation Add 477
Aggregation Delete 477
Aggregation Lookup 478
Aggregation Mode 478

6.10 Link Aggregation Control Protocol Command 480
LACP Configuration 480
LACP Mode 480
LACP Key 481
LACP Prio 481
LACP System Prio 482
LACP Role 482
LACP Status 483
LACP Statistics 483
LACP Timeout 484

6.11 LLDP Command 485
LLDP Configuration 485
LLDP Mode 485
LLDP Optional TLV 486
LLDP Interval 487
LLDP Hold 487
LLDP Delay 488
LLDP Reinit 488
LLDP Statistics 489
LLDP Info 489

6.12 LLDP MED Command 490
LLDP MED Configuration 490
LLDP MED Civic 490

LLDP MED ECS 491
LLDP MED Policy Delete 492
LLDP MED Policy Add 492
LLDP MED Port Policy 493
LLDP MED Coordinates 493
LLDP MED Datum 494
LLDP MED Fast 494
LLDP MED Info 495

6.13 EEE Command 496
EEE Configuration 496
EEE Mode 496
EEE Urgent Queues 497

6.14 Thermal Command 498
Thermal Prio_temp 498
Thermal Port_prio 498
Thermal Status 498
Thermal Configuration 499

6.15 PoE Command (NS3552-8P-2S only) 500
PoE Configuration 500
PoE Mode 500
PoE Priority 500
PoE Mamagement Mode 501
PoE Allocated Power 501
PoE Power Supply 501
PoE Status 502

6.16 Ethernet Virtual Connections Command 503
EVC Configuration 503
EVC Port DEI 503
EVC Port Tag 503
EVC Port Addr 504
EVC Port L2CP 504
EVC Policer 504
EVC Add 505
EVC Delete 505
EVC Lookup 506
EVC Status 506
EVC Statistics 506
EVC ECE Add 507
EVC ECE Delete 508

EVC ECE Lookup 508
EVC ECE Status 509

6.17 Ethernet Protection Switching Command 510
EPS Create 510
EPS Config 510
EPS Command 511
EPS State 511

6.18 Maintainence entity End Point Command 512
MEP Config 512
MEP Peer MEP 513
MEP Continuity Check Configuration 513
MEP Loss Measurement Configuration 513
MEP APS Configuration 514
MEP Client Configuration 514
MEP AIS Configuration 515
MEP LCK Configuration 515
MEP Link Trace Configuration 516
MEP Loop Back Configuration 516
MEP Delay Measurement Configuration 517
MEP Test Signal Configuration 518
MEP State 519
MEP Loss Measurement State 519
MEP Loss Measurement State Clear 519
MEP Link Trace State 520
MEP Loop Back State 520
MEP Delay Measurement State 520
MEP Delay Measurement State Clear 521
MEP Test Signal State 521
MEP Test Signal State Clear 521

6.19 Quality of Service Command 522
QoS Configuration 522
QoS Port Classification Class 522
QoS Port Classification DPL 523
QoS Port Classification PCP 523
QoS Port Classification DEI 524
QoS Port Classification Tag 524
QoS Port Classification Map 525
QoS Port Classification DSCP 525
QoS Port Policer Mode 526

QoS Port Policer Rate 526
QoS Port Policer Unit 527
QoS Port Policer Flow Control 527
QoS Port QueuePolicer Mode 528
QoS Port QueuePolicer Rate 528
QoS Port Scheduler Mode 529
QoS Port Scheduler Weight 529
QoS Port QueueShaper Mode 530
QoS Port QueueShaper Rate 530
QoS Port QueueShaper Excess 531
QoS Port TagRemarking Mode 531
QoS Port TagRemarking PCP 532
QoS Port TagRemarking DEI 532
QoS Port TagRemarking Map 533
QoS Port DSCP Translation 533
QoS Port DSCP Classification 534
QoS Port DSCP EgressRemark 535
QoS DSCP Map 535
QoS DSCP Translation 536
QoS DSCP Trust 536
QoS DSCP Classification Mode 536
QoS DSCP EgressRemap 537
QoS Storm Unicast 537
QoS Storm Multicast 538
QoS Storm Broadcast 538
QoS QCL Add 539
QoS QCL Delete 540
QoS QCL Lookup 541
QoS QCL Status 541
QoS QCL Refresh 541

6.20 Mirror Command 543

Mirror Configuration 543
Mirror Port 543
Mirror Mode 544

6.21 Configuration Command 545

Configuration Save 545
Configuration Load 545

6.22 Firmware Command 546

Firmware Load 546

Firmware IPv6 Load 546
Firmware Information 546
Firmware Swap 547

6.23 UPnP Command 548
UPnP Configuration 548
UPnP Mode 548
UPnP TTL 549
UPnP Advertising Duration 549

6.24 MVR Command 550
MVR Configuration 550
MVR Mode 550
MVR VLAN Setup 551
MVR VLAN Mode 551
MVR VLAN Port 551
MVR VLAN LLQI 552
MVR VLAN Channel 553
MVR VLAN Priority 553
MVR Immediate Leave 553
MVR Status 554
MVR Groups 554
MVR SFM 554

6.25 Voice VLAN Command 556
Voice VLAN Configuration 556
Voice VLAN Mode 556
Voice VLAN ID 557
Voice VLAN Agetime 558
Voice VLAN Traffic Class 558
Voice VLAN OUI Add 559
Voice VLAN OUI Delete 559
Voice VLAN OUI Clear 559
Voice VLAN OUI Lookup 560
Voice VLAN Port Mode 560
Voice VLAN Security 561
Voice VLAN Discovery Protocol 561

6.26 Ethernet Ring Protection Switching Command 562
ERPS Command 562
ERPS Version 563
ERPS Add 563
ERPS Reversion 564

ERPS VLAN Add 564
ERPS VLAN Delete 564
ERPS MEP 565
ERPS RPL Neighbour 565
ERPS RPL Owner 566
ERPS RPL Neighbour Clear 567
ERPS RPL Owner Clear 567
ERPS Hold Off Timeout 567
ERPS Guard-timeout 568
ERPS WRT-timeout 568
ERPS Delete 569
ERPS Topologychange 569
ERPS Configurationt 569

6.27 Loop Protect Command 570

Loop Protect Configuration 570
Loop Protect Mode 570
Loop Protect Transmit 570
Loop Protect Shutdown 571
Loop Protect Port Configuration 571
Loop Protect Port Mode 571
Loop Protect Port Action 572
Loop Protect Port Transmit 572
Loop Protect Status 572

6.28 IPMC Command 573

IPMC Configuration 573
IPMC Mode 573
IPMC Flooding 574
IPMC Leave Proxy 574
IPMC Proxy 575
IPMC SSM 575
IPMC VLAN Add 576
IPMC VLAN Delete 576
IPMC State 577
IPMC Querier 577
IPMC Compatibility 578
IPMC Fastleave 578
IPMC Throttling 579
IPMC Filtering 580
IPMC Router 580
IPMC Status 581

IPMC Group 581
IPMC Version 582
IPMC SFM 582
IPMC Parameter RV 582
IPMC Parameter QI 583
IPMC Parameter QRI 583
IPMC Parameter LLQI 584
IPMC Parameter URI 584

6.29 VLAN Control List Command 585
VCL MAC-based VLAN Configuration 585
VCL MAC-based VLAN Add 585
VCL MAC-based VLAN Delete 585
VCL Stasus 586
VCL Protocol-based VLAN Add Ethernet II 586
VCL Protocol-based VLAN Add SNAP 586
VCL Protocol-based VLAN Add LLC 587
VCL Protocol-based VLAN Delete Ethernet II 587
VCL Protocol-based VLAN Delete SNAP 587
VCL Protocol-based VLAN Delete LLC 588
VCL Protocol-based VLAN Add 588
VCL Protocol-based VLAN Delete 588
VCL Protocol-based VLAN Configuration 589
VCL IP Subnet-based Vlan Configuration 589
VCL IP Subnet-based Vlan Add 589
VCL IP Subnet-based Vlan Delete 590

6.30 SMTP Command 591
SMTP Configuration 591
SMTP Mode 591
SMTP Server 591
SMTP Auth 592
SMTP Auth_user 592
SMTP Auth_pass 593
SMTP Mail from 593
SMTP Mail Subject 593
SMTP Mail to 1 594
SMTP Mail to 2 594
SMTP Test 594

6.31 DIDO Command 595
DIDO DI Act 595

DIDO DI Desciption 595
DIDO DI Enable 596
DIDO DO Act 596
DIDO DO Enable 597
DIDO DO Port Alarm 597
DIDO DO Power Alarm 598
DIDO Fault Act 598
DIDO Fault Enable 599
DIDO Fault Port Alarm 599
DIDO Fault Power Alarm 599

6.32 Show Command 600

Show Access 600
Show ACL 600
Show Aggregation 600
Show ARP 600
Show Auth 600
Show DHCP Relay 601
Show EEE 601
Show HTTPs 601
Show IGMP 601
Show IP 602
Show LACP 602
Show Limit Control 602
Show LLDP 602
Show LLDP-MED 602
Show Loop Protect 603
Show MAC 603
Show Mirror 603
Show MVR 603
Show PoE 603
Show Port 604
Show Privilege 604
Show Private VLAN 604
Show QoS 604
Show SNMP 605
Show SSH 605
Show System 605
Show Timezone 605
Show UPnP 605
Show Users 606

Show VLAN 606
Show Voice VLAN 606
Show Firmware 606
Show STP 607

7. SWITCH OPERATION 608

7.1 Address Table 608

7.2 Learning 608

7.3 Forwarding & Filtering 608

7.4 Store-and-Forward 608

7.5 Auto-Negotiation 609

8. TROUBLE SHOOTING 610

APPENDEX A 612

A.1 Switch's Data RJ-45 Pin Assignments - 1000Mbps, 1000Base-T 612

A.2 10/100Mbps, 10/100Base-TX 612

APPENDEX B: GLOSSARY 614

1. INTRODUCTION

IFS Industrial Managed Switches (-40~75 degree C) are managed switches with multiple Gigabit copper ports or Gigabit SFP mini-GBIC slots with connective ability and robust layer 2 features.

NS3552-8P-2S Industrial 8-Port 10/100/1000T 802.3at PoE + 2 100/1000X SFP Managed Switch (-40~75 degrees C)

NS3550-2T-8S Industrial 8-port Gigabit Fiber (SFP) Industrial Managed Switch + 2 10/100/1000T (-40~75 degrees C)

The text "**Industrial Managed Switch**" mentioned in this User Guide represents the above two models. This manual represents multiple products which have similar features and functions, however there may be some differences between products such as the number or type of connectivity ports and PoE functions.

1.1 Packet Contents

Open the box of the Industrial Managed Switch and carefully unpack it. The box should contain the following items:

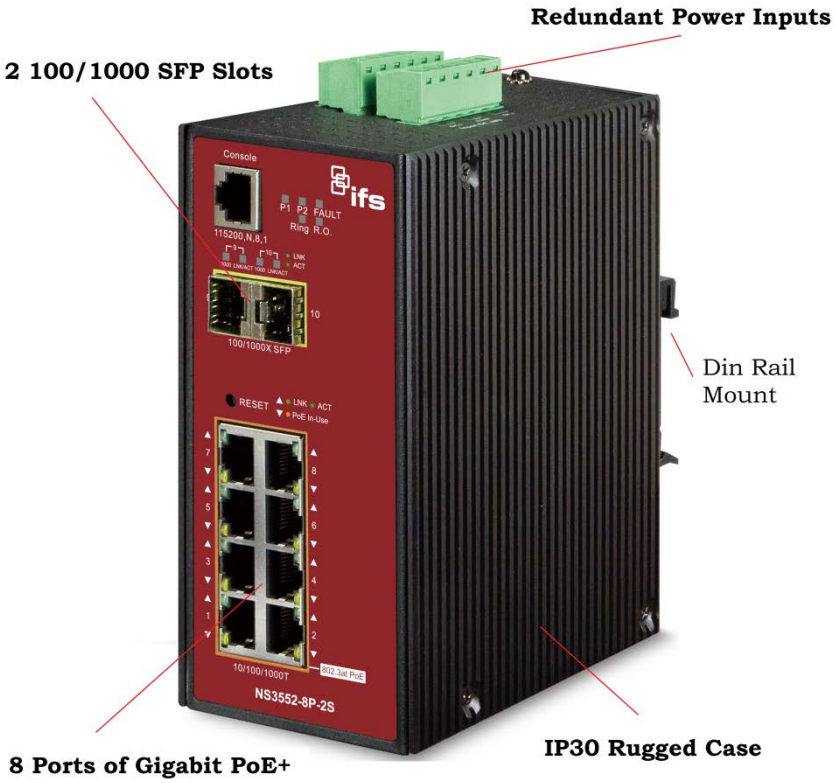
- ☑ **Industrial Managed Switch** x 1
- ☑ **Quick Installation Guide** x 1
- ☑ **User's Manual CD** x 1
- ☑ **DIN Rail Kit** x 1
- ☑ **Wall Mounting Kit** x 1
- ☑ **RS232 Console Cable** x 1
- ☑ **Dust Cap** x 11

If any of these are missing or damaged, please contact your dealer immediately. If possible, retain the carton including the original packing materials to enable you to repack the product in case there is a need to return it to us for repair.

1.2 Product Description

Environmentally Hardened Design

The Industrial Switches are equipped with rugged IP30 metal case for stable operation in heavy Industrial demanding environments. With IP30 industrial case protection, the switches provide a high level of immunity against electromagnetic interference and heavy electrical surges which are usually found on plant floors or in curb side traffic control cabinets. Being able to operate in wide temperature range from -40 to 75 degrees C, the Industrial Switches can be placed in almost any difficult environment. The Industrial Switches also allows for either DIN rail or wall mounting for efficient use of cabinet space.



Built-in Unique PoE Functions for Powered Devices Management (NS3552-8P-2S only)

As a managed PoE Switch for surveillance, wireless and VoIP network, the NS3552-8P-2S features three special PoE Management functions:

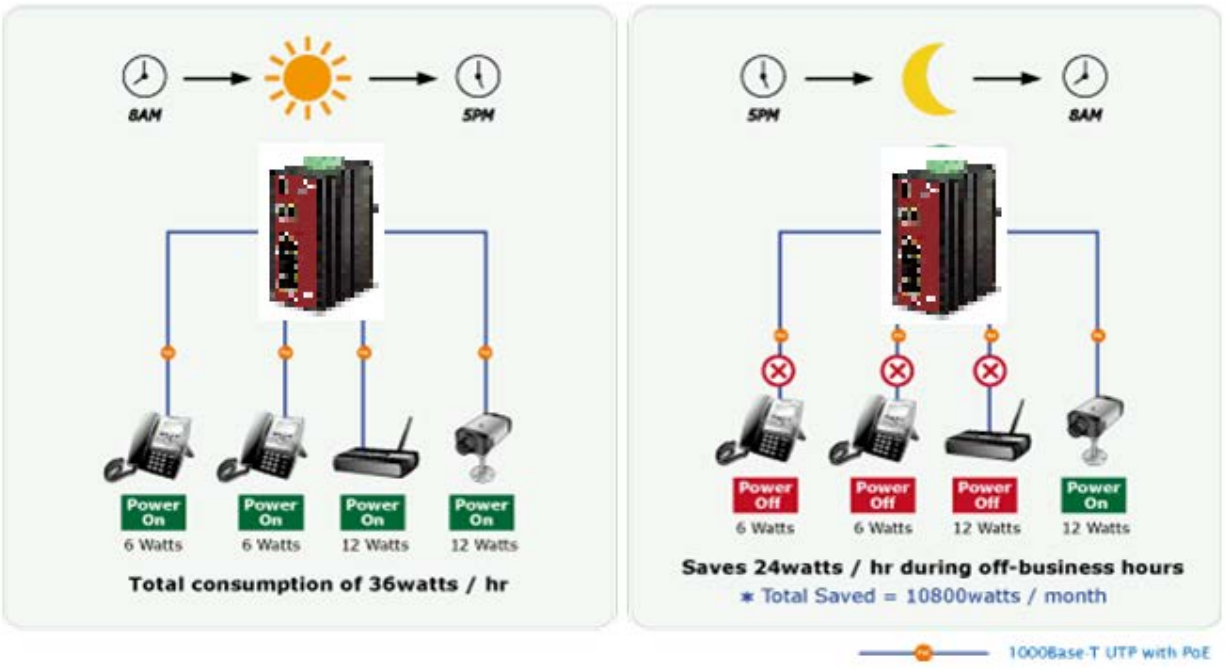
- **PD ALIVE Check**
- **Schedule Power Recycle**
- **SMTP/SNMP Trap Event Alert**
- **PoE Schedule**

Intelligent Alive Check for Powered Device

The NS3552-8P-2S can be configured to monitor connected PD (Powered Device) status in real-time via ping action. Once the PD stops working and responding, the NS3552-8P-2S will resume the PoE port power and bring the PD back to work. It will greatly enhance the network reliability through the PoE port resetting the PD's power source and reducing administrator management burden.

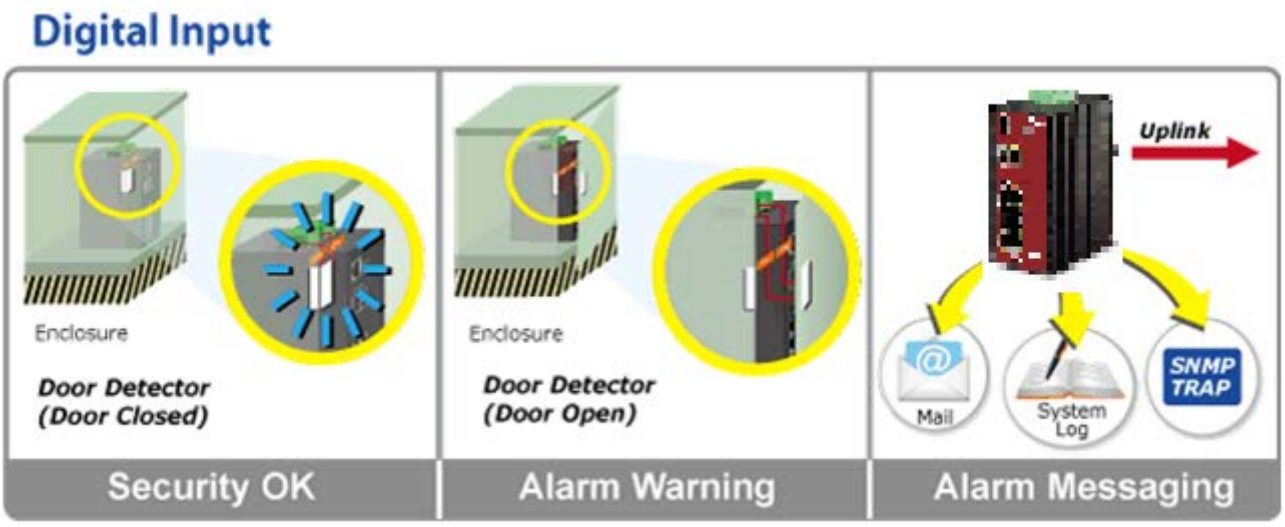
PoE Schedule for Energy Saving

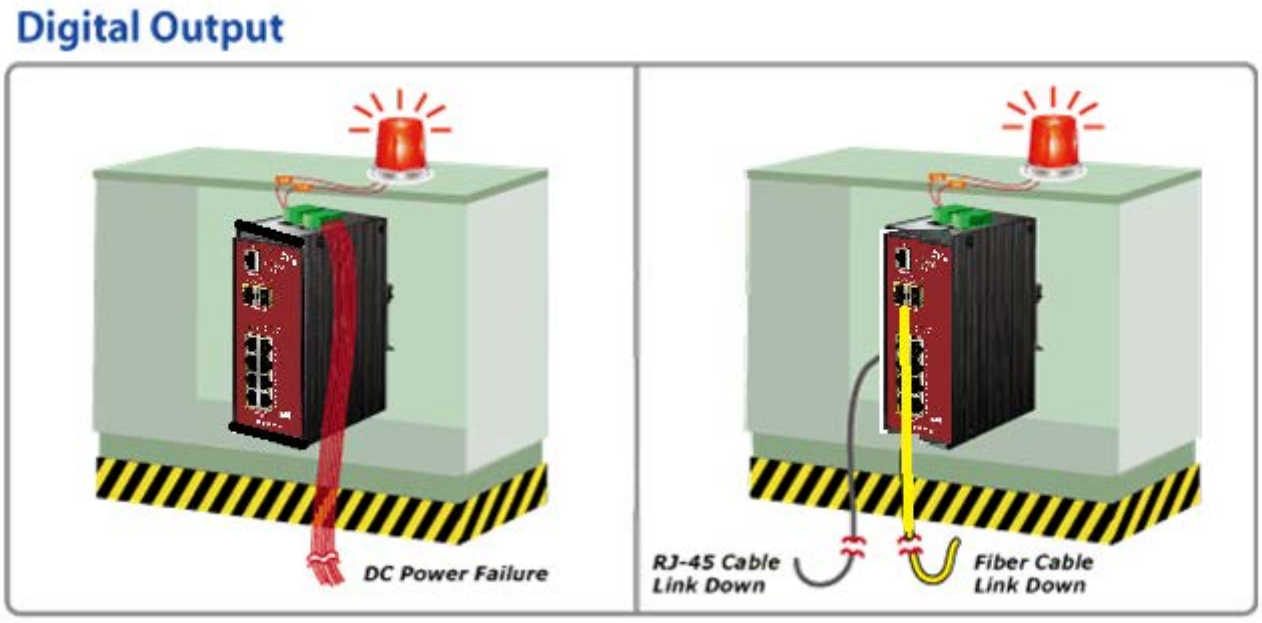
Under the trend of energy saving worldwide and contributing to environmental protection, the NS3552-8P-2S can effectively control the power supply besides its capability of giving high watts power. The built-in **"PoE schedule"** function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMB or Enterprise save power and money.



Digital Input and Digital Output for external Alarm

The Industrial Switches support Digital Input, and Digital Output on its front panel. This external alarm enables users to use Digital Input to detect, log external device status (such as door intrusion detector), and send event alarm to the administrators. The Digital Output could be used to alarm the administrators if the Industrial Switches port is link-down, link-up or power-failed.





Robust Layer 2 Feafures

The Industrial Switches can be programmed for advanced switch management function, such as dynamic port link aggregation, Q-in-Q VLAN, private VLAN, rapid spanning tree protocol, layer2 to layer4 QoS, bandwidth control and IGMP/MLD snooping. The NS3552-8P-2S provides 802.1Q tagged VLAN and the VLAN groups allowed will be maximally up to 255. The NS3552-8P-2S not only allows the operation of a high-speed trunk combining multiple ports, but also supports connection fail-over.

Efficient Management

For efficient management, the Industrial managed switch is equipped with console, web and SNMP management interfaces. With the built-in web-based management interface, the Industrial Switches offer an easy-to-use, platform independent management and configuration facility. The NS3552-8P-2S supports SNMP and it can be managed via any based on standard of SNMP v1 and v2 management software. For text-based management mode, the NS3552-8P-2S can be accessed via Telnet and the console port. Moreover, they also offer remote secure management by supporting **SSH, SSL** and **SNMPv3** connection which can be encrypted the packet content at each session.

Powerful Security

The Industrial Switches offer comprehensive layer2 to layer4 access control list (ACL) for enforcing security to the edge. It can be used to restrict to network access by denying packets based on source and destination IP address, TCP/UDP port number or defined typical network applications. Its protection mechanism also comprises 802.1x Port-based and MAC-based user and device authentication. With the private VLAN function, communication between edge ports can be prevented to ensure user privacy. The Industrial Switches also provide **DHCP Snooping, IP Source Guard and Dynamic ARP Inspection** functions to prevent IP snooping from attack and discard ARP packets with invalid MAC address. The network administrator can now construct highly secured corporate networks with considerably less time and effort than before.

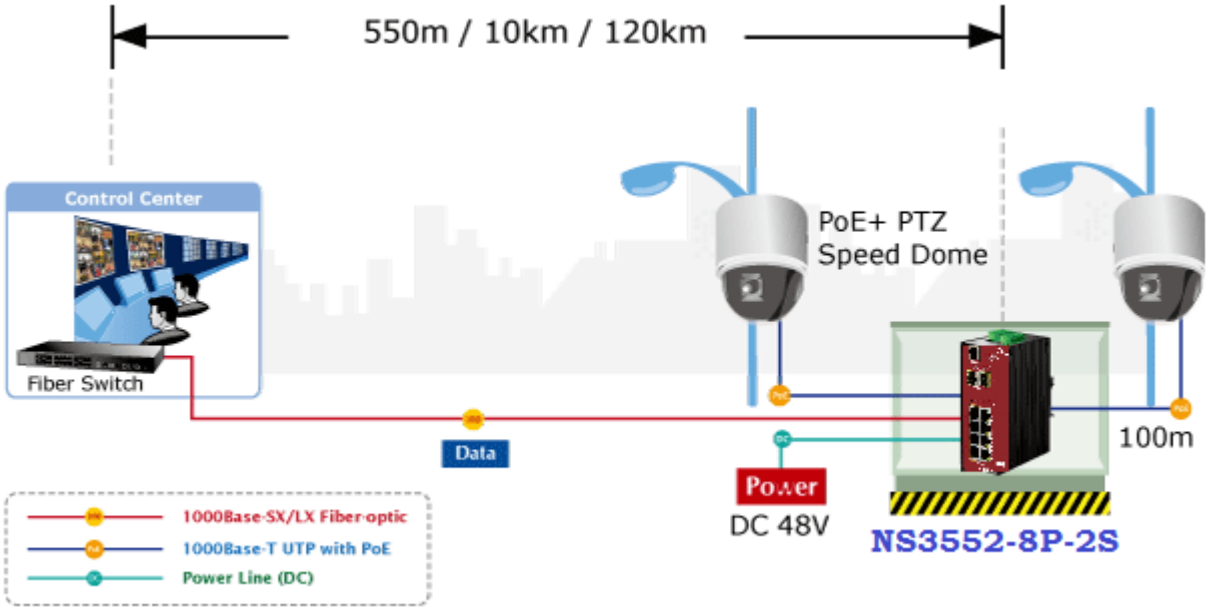
Flexibility and Extension Solution

The mini-GBIC slots built in the Industrial Switches supports dual speed that 100Base-FX and 1000Base-SX/LX SFP (Small Form-factor Pluggable) fiber-optic modules. Now the administrator can flexibly choose the suitable SFP transceiver according to not only the transmission distance, but also the transmission speed required. The distance can be extended from 550 meters to 2km (Multi-Mode fiber) up to above 10/20/30/40/50/70 kilometers (Single-Mode fiber or WDM fiber). They are well suited for applications within the enterprise data centers and distributions.

Perfect Integrafion Solution for Outdoor IP PoE Camera and NVR System

The NS3552-8P-2S provides 8 10/100/1000Mbps 802.3af/at PoE ports and can offer sufficient PoE power for 8 PoE IP cameras at the same time. In addition, with the 2-Port 100/1000Base-X SFP interfaces, the NS3552-8P-2S can connect to core fiber switch and send video stream to NVR and monitor center. Through the high performance switch architecture, the NS3552-8P-2S facilitates the recorded video files from the 8 PoE IP cameras to be saved in the NVR systems.

Furthermore, the NVR systems can be controlled and monitored both in the local LAN and the remote site via Internet. The NS3552-8P-2S undoubtedly brings an ideal, secure surveillance system at a lower total cost.



1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, **INSTALLATION**

The section explains the functions of the **Industrial Managed Switch** and how to physically install the **Industrial Managed Switch**.

Section 3, **SWITCH MANAGEMENT**

The section contains the information about the software function of the **Industrial Managed Switch**.

Section 4, **WEB CONFIGURATION**

The section explains how to manage the **Industrial Managed Switch** by Web interface.

Section 5, **COMMAND LINE INTERFACE**

The section describes how to use the Command Line interface (CLI).

Section 6, **CLI MODE**

The section explains how to manage the **Industrial Managed Switch** by Command Line interface.

Section 7, **SWITCH OPERATION**

The chapter explains how to do the switch operation of the **Industrial Managed Switch**.

Section 8, **TROUBLESHOOTING**

The chapter explains how to do troubleshooting of the **Industrial Managed Switch**.

Appendix A

The section contains cable information of the **Industrial Managed Switch**.

Appendix B

The section contains Glossary information of the **Industrial Managed Switch**.

1.4 Product Features

- **Physical Port**

NS3552-8P-2S

- **8-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45 with **IEEE 802.3af / 802.3at PoE** Injector
- **2 100/1000Base-X mini-GBIC/SFP** slots, SFP type auto detection
- One RJ-45 console interface for basic management and setup

NS3550-2T-8S

- **2-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45
- **8 100/1000Base-X mini-GBIC/SFP** slots, SFP type auto detection
- One RJ-45 console interface for basic management and setup NS3552-8P-2S
- **8-Port 10/100/1000Base-T** Gigabit Ethernet RJ-45 with **IEEE 802.3af / 802.3at PoE** Injector
- **2 100/1000Base-X mini-GBIC/SFP** slots, SFP type auto detection
- One RJ-45 console interface for basic management and setup

- **Power over Ethernet (NS3552-8P-2S ONLY)**
  - Complies with IEEE 802.3af / IEEE 802.3at Power over Ethernet / End-Span PSE (NS3552-8P-2S)
  - Complies with IEEE 802.3af Power over Ethernet / End-Span PSE
  - Up to 8 IEEE 802.3af / 802.3at devices powered (NS3552-8P-2S)
  - Supports PoE Power up to 15.4watts or 30.8 watts for each PoE port (NS3552-8P-2S)
  - Auto detect powered device (PD)
  - Circuit protection prevents power interference between ports
  - Remote power feeding up to 100m
  - PoE Management features:
    - IEEE 802.3af and IEEE 802.3at mode switch control (NS3552-8P-2S)
    - Total PoE power budget control
    - Per port PoE function enable/disable
    - PoE Admin-mode control
    - PoE Port Power feeding priority
    - Per PoE port power limit
    - PD classification detection
    - Temperature Threshold Control
    - PoE Usage Threshold Control
    - PD Alive Check
    - PoE Schedule
    - PD Power Recycling Schedule

- **Industrial Case / Installation**
  - IP30 aluminum metal case protection
  - DIN rail and wall mount design
  - 48V DC, redundant power with polarity reverse protect function
  - Supports EFT protection 6000 VDC for power line
  - Supports 6000 VDC Ethernet ESD protection
  - -40 to 75 degrees C operating temperature

- **Digital Input / Digital Output**
  - 2 Digital Input (DI)
  - 2 Digital Output (DO)
  - Integrate sensors into auto alarm system
  - Transfer alarm to IP network via email and SNNP trap

- **Layer 2 Features**
  - Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x PAUSE frame flow control (full-duplex)
  - High performance of Store-and-Forward architecture and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
  - Storm Control support:
    - Broadcast / Multicast / Unicast
  - Supports **VLAN**
    - IEEE 802.1Q Tagged VLAN
    - Up to 255 VLANs groups, out of 4094 VLAN IDs
    - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
    - Private VLAN Edge (PVE)
    - Protocol-based VLAN
    - MAC-based VLAN
    - Voice VLAN
  - Supports **Spanning Tree Protocol**
    - STP, IEEE 802.1D Spanning Tree Protocol
    - RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
    - MSTP, IEEE 802.1s Multiple Spanning Tree Protocol, spanning tree by VLAN
    - BPDU Guard
  - Supports **Link Aggregation**
    - 802.3ad Link Aggregation Control Protocol (LACP)
    - Cisco ether-channel (Static Trunk)
    - Maximum 5 trunk groups, up to 8 ports per trunk group
    - Up to 16Gbps bandwidth(Duplex Mode)
  - Provides Port Mirror (1-to-1)
  - Port Mirroring to monitor the incoming or outgoing traffic on a particular port
  - Loop protection to avoid broadcast loops
  - Supports E.R.P.S. **(Ethernet Ring Protection Switching)**

- **Quality of Service**
  - Ingress Shaper and Egress Rate Limit per port bandwidth control
  - 8 priority queues on all switch ports
  - Traffic classification:
    - IEEE 802.1p CoS
    - IP TOS / DSCP / IP Precedence
    - IP TCP/UDP port number
    - Typical network application

- Strict priority and Weighted Round Robin (WRR) CoS policies
- Supports QoS and In/Out bandwidth control on each port
- Traffic-policing policies on the switch port
- DSCP remarking

- **Multicast**
  - Supports IGMP Snooping v1, v2 and v3
  - Supports MLD Snooping v1 and v2
  - Querier mode support
  - IGMP Snooping port filtering
  - MLD Snooping port filtering
  - MVR (Multicast VLAN Registration)

- **Security**
  - IEEE 802.1x Port-based / MAC-based network access authentication
  - Built-in RADIUS client to co-operate with the RADIUS servers
  - TACACS+ login users access authentication
  - RADIUS / TACACS+ users access authentication
  - IP-based Access Control List (ACL)
  - MAC-based Access Control List
  - Source MAC / IP address binding
  - DHCP Snooping to filter untrusted DHCP messages
  - Dynamic ARP Inspection discards ARP packets with invalid MAC address to IP address binding
  - IP Source Guard prevents IP spoofing attacks
  - Auto DoS rule to defend DoS attack
  - IP address access management to prevent unauthorized intruder

- **Management**
  - Switch Management Interfaces
    - Console / Telnet Command Line Interface
    - Web switch management
    - SNMP v1 and v2c switch management
    - SSH / SSL and SNMP v3 secure access
  - Four RMON groups (history, statistics, alarms, and events)
  - **IPv6** IP Address / NTP / DNS management
  - Built-in Trivial File Transfer Protocol (TFTP) client
  - BOOTP and DHCP for IP address assignment
  - Firmware upload/download via HTTP / TFTP
  - DHCP Relay
  - DHCP Option82
  - User Privilege levels control

- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) Protocol
- SFP-**DDM** (Digital Diagnostic Monitor)
- Cable Diagnostic technology provides the mechanism to detect and report potential cabling issues
- Reset button for system reboot or reset to factory default
- IFS Smart Discovery Utility for deploy management

1.5 Product Specifications

Product	NS3552-8P-2S	NS3550-2T-8S
Hardware Specification		
Copper Ports	2 10/ 100/1000Base-T RJ-45s	2 10/100/1000Base-T Ethernet interface
SFP/mini-GBIC Slots	8 1000Base-SX/LX/BX SFP interfaces Compatible with 100Base-FX SFP	8 100/1000Base-SX/LX mini-GBIC SFP slots
Console	1 x RJ-45-to-RS-232 serial port (115200, 8, N, 1)	
Switch Architecture	Store-and-Forward	Store-and-Forward
Switch Fabric	20Gbps / non-blocking	20Gbps / non-blocking
Throughput (packet per second)	14.8Mpps@ 64Bytes packet	14.8Mpps
Address Table	8K entries, automatic source address learning and ageing	8K entries, automatic source address learning and ageing
Share Data Buffer	4Mbits	
Flow Control	IEEE 802.3x Pause Frame for Full-Duplex Back pressure for Half-Duplex	IEEE 802.3x Pause Frame for Full-Duplex. Back pressure for Half-Duplex
Jumbo Frame	9Kbytes	9Kbytes
Reset Button	< 5 sec: System reboot > 10 sec: Factory Default	< 5 sec: System reboot > 10 sec: Factory Default
ESD Protection	6KV DC	6KV DC
EFT Protection	6KV DC	6KV DC
Enclosure	IP30 Aluminum Metal Case	IP30 Aluminum Metal Case
Installation	DIN Rail Kit and Wall Mount Kit	DIN Rail Kit and Wall Mount Kit
Connector	Removable 6-pin terminal block for power input Pin 1/2 for Power 1; Pin 3/4 for fault alarm; Pin 5/6 for Power 2 Removable 6-pin terminal block for DI/DO interface Pin 1/2 for DI 1 & 2; Pin 3/4 for DO 1 & 2; Pin 5/6 for GND	
Alarm	One relay output for power failure. Alarm Relay current carry ability: 1A @ DC 24V	One relay output for power fail. Alarm Relay current carry ability: 1A @ DC 24V
DI/DO	2 Digital Input (DI): Level 0: -24V~2.1V (±0.1V) Level 1: 2.1V~24V (±0.1V) Input Load to 24V DC, 10mA max. 2 Digital Output (DO): Open collector to 24VDC, 100mA max.	
LED Indicator	System: Power 1 (Green) Power 2 (Green) Fault Alarm (Green) Ring (Green) Ring Owner (Green) Per 10/100/1000T RJ-45 Ports: PoE In-Use (Orange) (NS3552-8P-2S only) LNK/ACT (Green) Per SFP Interface: 1000 (Orange) LNK/ACT (Green)	System: Power 1 (Green) Power 2 (Green) Fault Alarm (Green) Ring (Green) R.O. (Green) Per 10/100/1000T RJ-45 Ports: 1000 (Green) 10/100, LNK/ACT (Orange) Per SFP Interface: 1000 LNK/ACT (Green) 100 LNK/ACT (Orange)
Dimensions (W x D x H)	152 x 107x 72mm	152 x 107x 72mm
Weight	1684g	1036g
Power Requirements	DC 48V	DC 12 to 48V, AC 24V Power Adapter
Power	At/31.9 watts / 108.78BTU (Full loading without PoE	13.92 Watts / 47.76BTU (Full loading)

Consumption	function) 306 watts / 1043.46BTU (Full loading with PoE function) (NS3552-8P-2S only)	
Power Over Ethernet (NS3552-8P-2S only)		
PoE Standard	IEEE 802.3af / IEEE 802.3at Power over Ethernet / PSE	
PoE Power Supply Type	End-Span	
PoE Power Output	Per Port 56V DC, 350mA . Max. 15.4 watts (IEEE 802.3af) Per Port 56V DC, 590mA. Max. 30 watts (IEEE 802.3at)	
Power Pin Assignment	1/2(+), 3/6(-)	
PoE Power Budget	270W maximum (depending on power input)	
Max. number of Class 2 PD	8	
Max. number of Class 3 PD	8	
Max. number of Class 4 PD	8	
Layer 2 Function		
Basic Management Interfaces	Console, Telnet, Web Browser, SNMPv1, v2c	Web Browser, Remote Telnet, SNMPv1, v2c
Secure Management Interfaces	SSH, SSL, SNMP v3	SSH, SSL, SNMP v3
Port Configuration	Port disable/enable Auto-Negotiation 10/100/1000Mbps full and half duplex mode selection Flow Control disable / enable Power saving mode control	Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Auto-detection / Forced 100/1000Mbps SFP Fiber transceiver speed. Flow Control disable / enable Power saving mode control
Port Status	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status, trunk status.	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status, trunk status.
Port Mirroring	TX / RX / Both 1 to 1 monitor	TX / RX / Both Many to 1 monitor
VLAN	802.1Q Tagged Based VLAN, up to 255 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) MAC-based VLAN Protocol-based VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4094 VLAN IDs	802.1Q Tagged Based VLAN ,up to 255 VLAN groups Q-in-Q tunneling Private VLAN MAC-based VLAN Protocol-based VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4095 VLAN IDs
Link Aggregation	IEEE 802.3ad LACP / Static Trunk Supports 5 groups of 8-Port trunk support	IEEE 802.3ad LACP / Static Trunk Support 5 groups of 10-Port trunk support
QoS	Traffic classification based, Strict priority and WRR 8-Level priority for switching - Port Number	Traffic classification based, Strict priority and WRR 8-level priority for switching - Port Number

	- 802.1p priority - 802.1Q VLAN tag - DSCP/TOS field in IP Packet	- 802.1p priority - 802.1Q VLAN tag - DSCP field in IP Packet
IGMP Snooping	IGMP (v1/v2/V3) Snooping, up to 255 multicast Groups IGMP Querier mode support	IGMP (v1/v2/V3) Snooping, up to 255 multicast Groups IGMP Querier mode support
MLD Snooping	MLD (v1/v2) Snooping, up to 255 multicast Groups MLD Querier mode support	MLD (v1/v2) Snooping, up to 255 multicast Groups MLD Querier mode support
Access Control List	IP-based ACL / MAC-based ACL Up to 123 entries	IP-Based ACL / MAC-Based ACL Up to 256 entries
Bandwidth Control	Per port bandwidth control Ingress: 500Kb~1000Mbps Egress: 500Kb~1000Mbps	Per port bandwidth control Ingress: 500Kb~1000Mbps Egress: 500Kb~1000Mbps
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB RFC-2819 RMON MIB (Group 1, 2, 3 and 9) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC-2933 IGMP-STD-MIB RFC3411 SNMP-Frameworks-MIB IEEE 802.1X PAE LLDP MAU-MIB	RFC-1213 MIB-II RFC-2236 IGMPv2 RFC-2710 MLDv1 RFC-3376 IGMPv3 RFC-2879 RMON 1, 2, 3, 9 RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB RFC-2819 RMON MIB (Group 1, 2, 3 and 9) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC3411 SNMP-Frameworks-MIB IEEE 802.1X PAE IF-MIB LLDP MAU-MIB
Standards Conformance		
Regulation Compliance	FCC Part 15 Class A, CE	FCC Part 15 Class A, CE
Stability Testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/100Base-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1D Spanning tree protocol IEEE 802.1w Rapid spanning tree protocol IEEE 802.1s Multiple spanning tree protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet (NS3552-8P-2S)	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX / 100Base-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ab LLDP

	RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2	
Environment		
Operating Temperature	-40 ~ 75 degrees C	-40 ~ 75 degrees C
Storage Temperature	-40 ~ 85 degrees C	-40 ~ 85 degrees C
Humidity	5 ~ 95% (Non-condensing)	5 ~ 95% (Non-condensing)

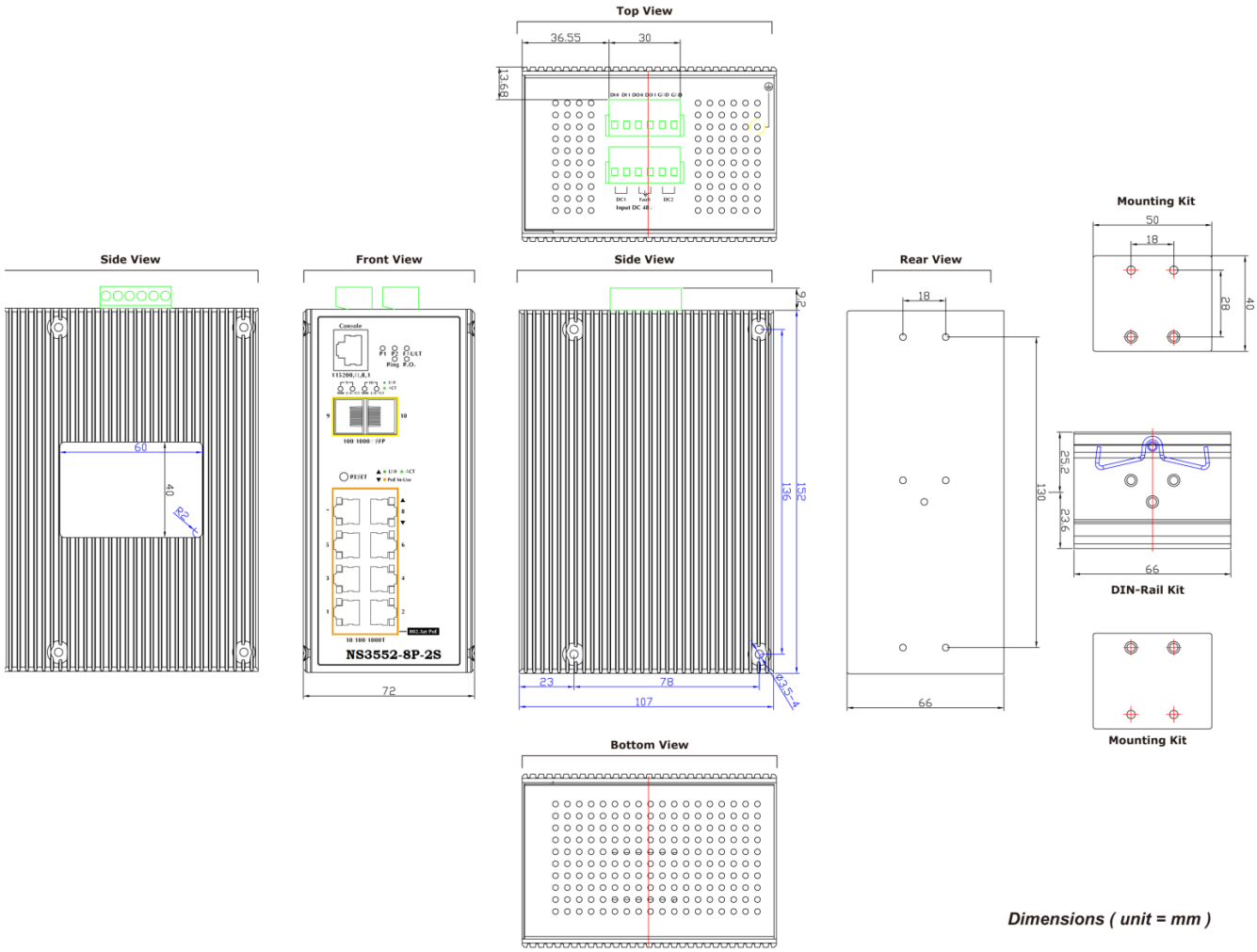
2. INSTALLATION

2.1 Hardware Descriptions

The Managed Switch provides three different running speeds – 10Mbps, 100Mbps and 1000Mbps – in the same Switch and automatically distinguishes the speed of incoming connection. This section describes the hardware features of the Managed Switch. For easier management and control of the Managed Switch, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit's LED indicators. Before connecting any network device to the Managed Switch, read this chapter carefully.

2.1.1 Physical Dimensions

- **Industrial Switches**
  - Dimensions (W x D x H) : 72 x 107 x 152 mm



Dimensions (unit = mm)

2.1.2 Front Panel

Figure 2-1 & 2-2 shows the front panels of **Industrial Managed Switch**.

Figure 2-2: NS3552-8P-2S Switch Front Panel

■ Reset Button

At the left of the front panel, the reset button is designed for rebooting the **Industrial Managed Switch** without turning off and on the power. It also can reset the **Industrial Managed Switch** to factory default mode.

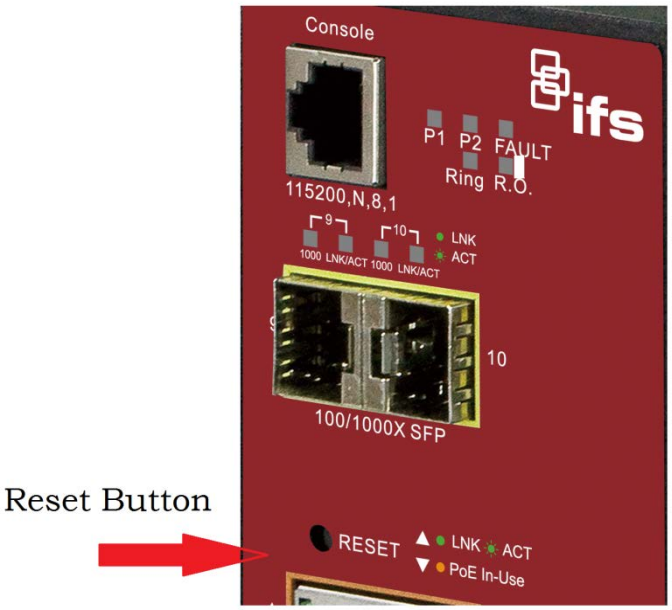


Figure 2-3: Reset button of **Industrial Managed Switch**

Reset Button Pressed and Released	Function
< 5 sec: System Reboot	Reboot the Industrial Managed Switch
> 10 sec: Factory Default	Reset the Industrial Managed Switch to Factory Default configuration. The Industrial Managed Switch will then reboot and load the default settings as below: ◦ Default Username: **admin** ◦ Default Password: **admin** ◦ Default IP address: **192.168.0.100** ◦ Subnet mask: **255.255.255.0** ◦ Default Gateway: **192.168.0.254**

2.1.3 LED Indicators

■ **System**

LED	Color	Function
P1	**Green**	**Lights** to indicate that the Switch is powered on by DC1 input.
P2	**Green**	**Lights** to indicate that the Switch is powered on by DC2 input.
Fault	**Green**	**Lights** to indicate that Switch DC or port has failed.
Ring*	**Green**	**Lights** to indicate that the ERPS Ring has been created successfully.
R.O.*	**Green**	**Lights** to indicate that Switch has enabled Ring Owner.

* = features to be expected in the future

■ **Per 10/100/1000Mbps port with PoE**

LED	Color	Function
10/100/1000 LNK/ACT	**Green**	**Lights** to indicate the port is running in **10/100/1000Mbps** speed and successfully established. **Blink**: indicates that the switch is actively sending or receiving data over that port.
PoE In-Use	**Orange**	**Lights**: To indicate the port is providing 48/56V DC in-line power. **Off:** To indicate the connected device is not a PoE Powered Device (PD).

■ **Per SFP Interface (Port-9, Port-10 mini-GBIC)**

LED	Color	Function	
LNK / ACT	**Green**	**Light**	Indicates the link through that port is successfully established.
		Blink	Indicates that the Switch is actively sending or receiving data over that port.
1000	**Orange**	**Light**	Indicates that the port is successfully connecting to the network at 1000Mbps.
		Off	Indicates that the port is successfully connecting to the network at 100Mbps.

2.1.4 Wiring the Power Input

The 6-contact terminal block connector on the top panel of the Industrial Managed Switch is used for two DC redundant power inputs. Please follow the steps below to insert the power wire.

1. Insert positive / negative DC power wires into the contacts 1 and 2 for DC POWER 1, or 5 and 6 for DC POWER 2.

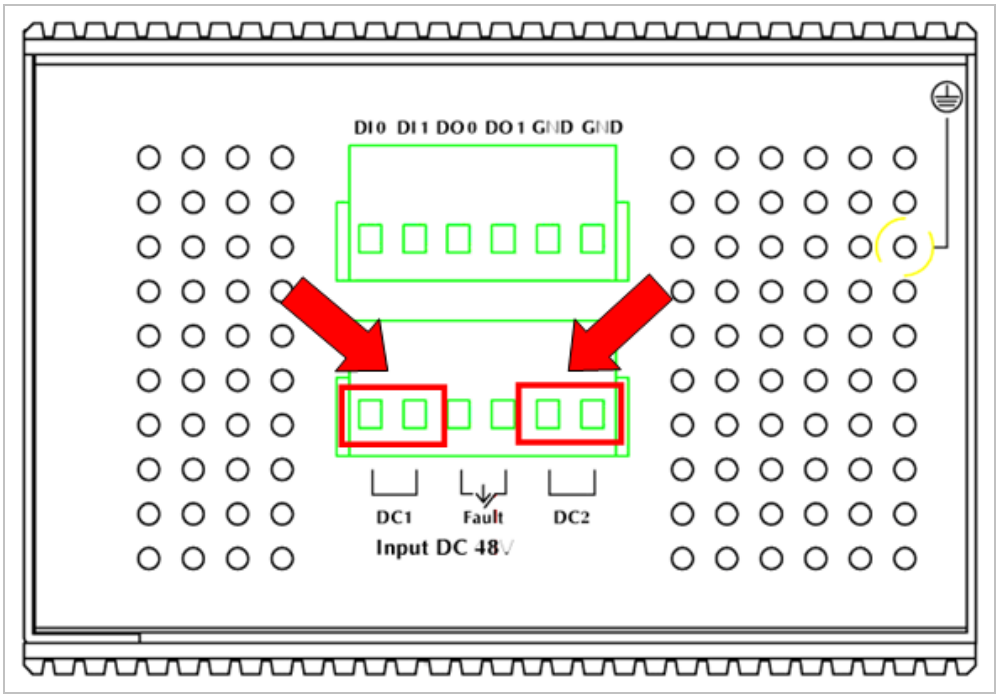


Figure 2-4: NS3552-8P-2S Upper Panel

2. Tighten the wire-clamp screws for preventing the wires from loosening.

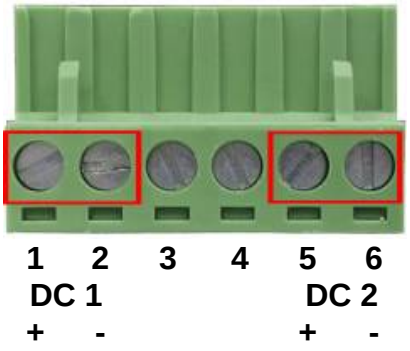


Figure 2-5 6-Pin Terminal Block Power Wiring Input

Note

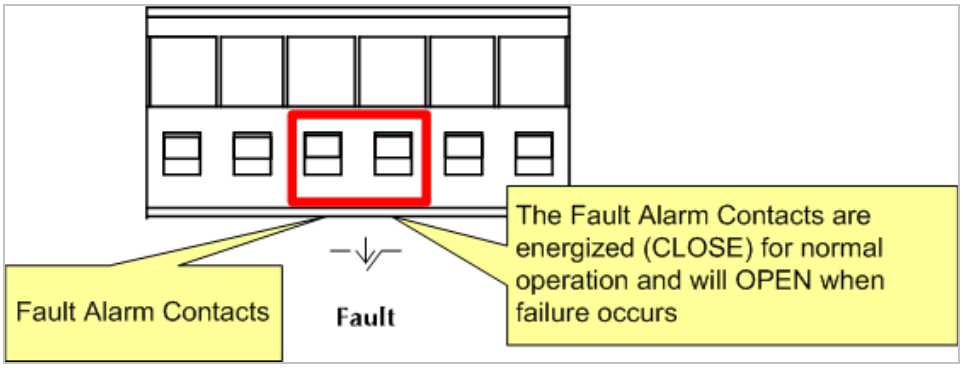
1. The wire gauge for the terminal block should be in the range of 12 ~ 24 AWG.
2. When performing any of the procedures like inserting the wires or tighten the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

2.1.5 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle (3 & 4) of the terminal block connector as the picture shows below. Inserting the wires,

the **Industrial Managed Switch** will detect the fault status of the power failure, or port link failure (available for managed model).

The following illustration shows an application example for wiring the fault alarm contacts


The Fault Alarm Contacts are energized (CLOSE) for normal operation and will OPEN when failure occurs
Fault Alarm Contacts
Fault

Insert the wires into the fault alarm contacts

Note

1. The wire gauge for the terminal block should be in the range of 12 ~ 24 AWG.
2. When performing any of the procedures like inserting the wires or tighten the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

2.1.6 Wiring the Digital Input / Output

The 6-contact terminal block connector on the rear panel of NS3552-8P-2S is used for Digital Input and Digital Output. Please follow the steps below to insert wire.

1. The NS3552-8P-2S offers two DI and DO groups. 1 and 2 are DI groups, 3 and 4 are DO groups and 5 and 6 are GND (ground).

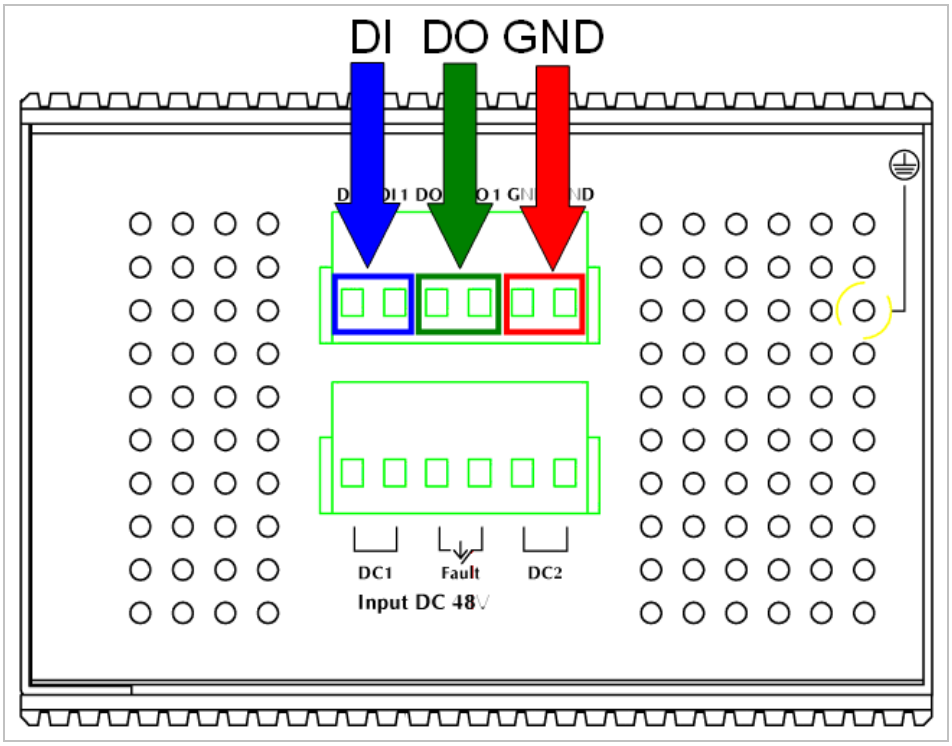


Figure 2-6 Wiring the Redundant Power Inputs

2. Tighten the wire-clamp screws for preventing the wires from loosening.

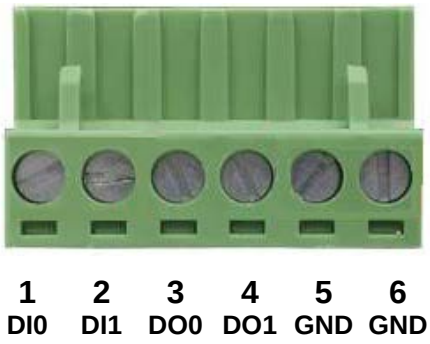


Figure 2-7 6-Pin Terminal Block DI / DO Wiring Input

3. There are two Digital Input groups for you to monitor two different devices. The following topology shows how to wire DI0 and DI1.

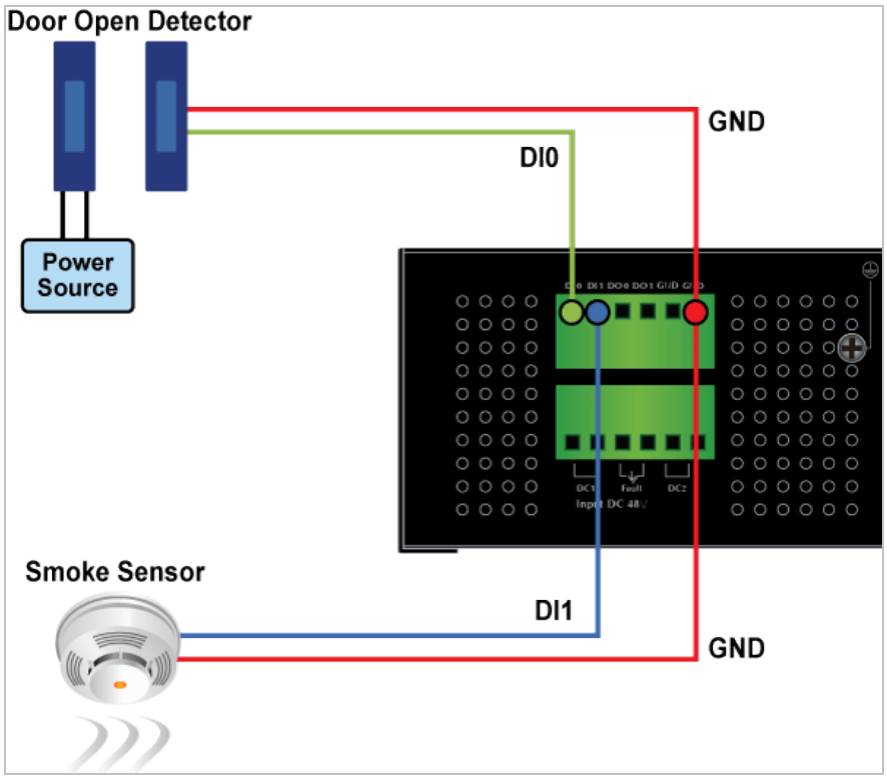


Figure 2-8 Wires DI0 and DI1 to Open Detector

4. There are two Digital Output groups for you to sense the Industrial Switches port failure or power failure and issue a high or low signal to external device. The following topology shows how to wire DO0 and DO1.

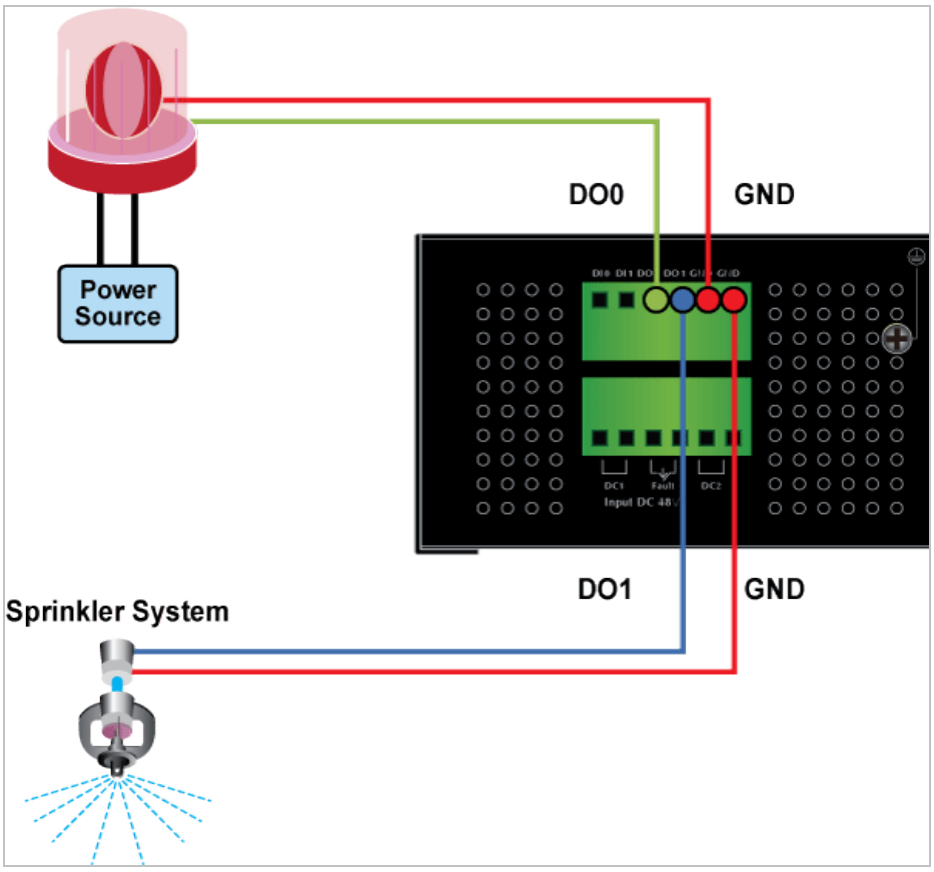


Figure 2-9 Wires DO0 and DO1 to Open Detector

2.2 Install the Industrial Managed Switch

This section describes how to install the **Industrial Managed Switch** and make connections to it. Please read the following topics and perform the procedures in the order being presented. To install your **Industrial Managed Switch** on a desktop or shelf, simply complete the following steps.

In this paragraph, we will describe how to install the **Industrial Managed Switch** and the installation points attended to it.

2.2.1 Installation Steps

1. **Unpack the Industrial Managed Switch**
2. **Check if the DIN-Rail is screwed on the Industrial Managed Switch or not**. If the DIN-Rail is not screwed on the **Industrial Managed Switch**, please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If users want to wall-mount the **Industrial Managed Switch**, please refer to the **Wall Mount Plate Mounting** section for wall-mount plate installation**.**
3. **To hang the Industrial Managed Switch on the DIN-Rail track or wall.**
4. **Power on the Industrial Managed Switch**. Please refer to the **Wiring the Power Inputs** section for knowing the information about how to wire the power. The power LED on the **Industrial Managed Switch** will light up. Please refer to the **LED Indicators** section for indication of LED lights**.**
5. **Prepare the twisted-pair, straight through Category 5 cable for Ethernet connection.**
6. **Insert one side of RJ-45 cable (category 5) into the Industrial Managed Switch Ethernet port** (RJ-45 port) and another side of RJ-45 cable (category 5) to the network device's Ethernet port (RJ-45 port), ex: Switch PC or Server. The UTP port (RJ-45) LED on the **Industrial Managed Switch** will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication**.**

Make sure that the connected network devices support MDI/MDI-X if it does not support, or use the crossover category-5 cable.

7. **When all connections are set and LED lights all show normal, the installation is completed.**

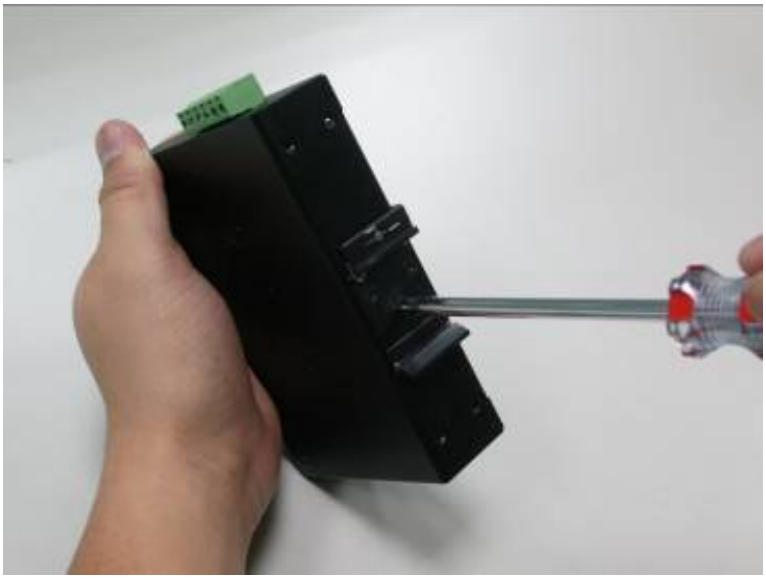
2.2.2 DIN-Rail Mounting

This section describes how to install the **Industrial Managed Switch**.

There are two methods to install the **Industrial Managed Switch** -- DIN-Rail Mounting and Wall Mount Plate Mounting. Please read the following topics and perform the procedures in the order being presented.

In the installation steps below, this Manual use NS3550-2T-8S (IFS 8 Port Industrial Gigabit Switch) as the example. However, the steps for IFS Industrial Gigabit PoE+ Switch are similar.

Step 1: Screw the DIN-Rail on the **Industrial Managed Switch**.



Step 2: Lightly insert the bottom of the switch into the track.

Step 3: Check if the DIN-Rail is tightly on the track.

Please refer to following procedures to remove the **Industrial Managed Switch** from the track.

Step 1: Lightly pull out the bottom of the switch for removing it from the track.

2.2.3 Wall Mount Plate Mounting

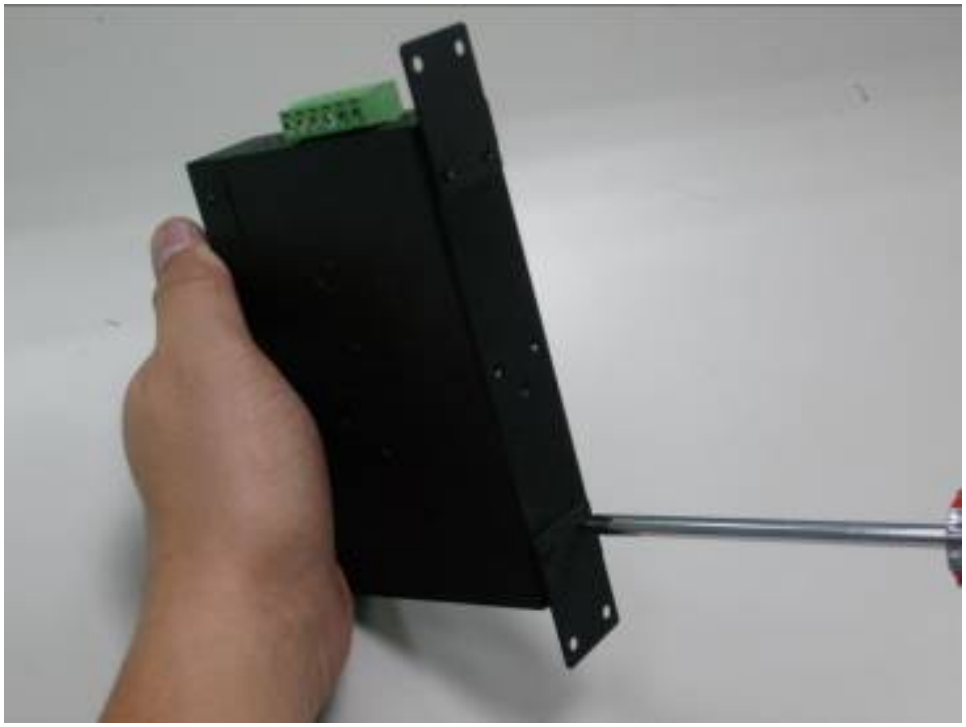
To install the **Industrial Managed Switch** on the wall, please follow the instructions below.

Note

In the installation steps below, this Manual use NS3550-2T-8S (IFS 8 Port Industrial Gigabit Switch) as the example. However, the steps for IFS Industrial Gigabit PoE+ Switch are similar.

Step 1: To remove the **Industrial Managed Switch** from the DIN-Rail, use the screwdriver to loosen the screws and remove the DIN-Rail.

Step 2: Place the wall mount plate on the rear panel of the **Industrial Managed Switch**.



Step 3: Use the screws to screw the wall mount plate on the **Industrial Managed Switch**.

Step 4: Use the hook holes at the corners of the wall mount plate to hang the **Industrial Managed Switch** on the wall.

Step 5: To remove the wall mount plate, reverse steps above.

2.3 Cabling

- **10/100/1000Base-T and 100Base-FX / 1000Base-SX/LX**

All 10/100/1000Base-T ports come with Auto-Negotiation capability. They automatically support 1000Base-T, 100Base-TX and 10Base-T networks. Users only need to plug a working network device into one of the 10/100/1000Base-T ports, and then turn on the **Industrial Managed Switch**. The port will automatically run in 10Mbps, 20Mbps, 100Mbps or 200Mbps and 1000Mbps or 2000Mbps after the negotiation with the connected device.

The **Industrial Managed Switch** has eight SFP interfaces that support 100/1000Mbps dual speed mode (optional multi-mode/ single-mode 100Base-FX/1000Base-SX/LX SFP module)

- **Cabling**

Each 10/100/1000Base-T port uses RJ-45 sockets -- similar to phone jacks -- for connection of unshielded twisted-pair cable (UTP). The IEEE 802.3/802.3u 802.3ab Fast/Gigabit Ethernet standard requires Category 5 UTP for 100Mbps 100Base-TX. 10Base-T networks can use Cat.3, 4, 5 or 1000Base-T use 5/5e/6 UTP (see table below). Maximum distance is 100meters (328 feet). The 100Base-FX/1000Base-SX/LX SFP slot is used as LC connector with optional SFP module. Please see table below and know more about the cable specifications.

Port Type	Cable Type	Connector
10Base-T	Cat 3, 4, 5, 2-pair	RJ-45
100Base-TX	Cat.5 UTP, 2-pair	RJ-45
1000Base-T	Cat.5/5e/6 UTP, 2-pair	RJ-45
100Base-FX	50 / 125µm or 62.5 / 125µm multi-mode 9 / 125µm single-mode	LC (Multi / Single mode)
1000Base-SX/LX	50 / 125µm or 62.5 / 125µm multi-mode 9 / 125µm single-mode	LC (Multi / Single mode)

Any Ethernet devices like hubs/PCs can connect to the **Industrial Managed Switch** by using straight-through wires. The two 10/100/1000Mbps ports are auto-MDI/MDI-X , which can be used on straight-through or crossover cable.

2.3.1 Installing the SFP Transceiver

The sections describe how to insert an SFP transceiver into an SFP slot. The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the **Industrial Managed Switch** as the Figure 2-9 appears.

Figure 2-9: Plugging in the SFP Transceiver

- **Approved IFS SFP Transceivers**

  IFS **Industrial Managed Switch** supports 100/1000 dual mode with both Single mode and Multi-mode SFP transceiver. The following list of approved IFS SFP transceivers is correct at the time of publication:

  Gigabit SFP Transceiver Modules

S30-1SLC/A-10	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1310nm/1550nm, 10km , A End
S30-1SLC/A-20	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1310nm/1550nm, 20km, A End
S30-1SLC/A-60	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1310nm/1550nm, 60km, A End
S30-1SLC/B-10	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1550nm/1310nm, 10km , B End
S30-1SLC/B-20	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1550nm/1310nm, 20km, B End
S30-1SLC/B-60	SFP, LC Connector, Single Mode, Gigabit, 1 fiber, 1550nm/1310nm, 60km, B End
S30-2MLC	SFP, LC Connector, Multi-Mode, Gigabit, 2 fiber,850nm/850nm, 550m
S30-2MLC-2	SFP, LC Connector, Multi-Mode, Gigabit, 2 fiber,1310nm/1310nm, 2km
S30-2SLC-10	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 10km

S30-2SLC-30	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 30km

S30-2SLC-70	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1550nm/1550nm, 70km
S30-RJ	SFP, RJ-45, Gigabit, 100m
S35-2MLC	SFP, LC Connector, Multi-Mode, Gigabit, 2 fiber,850nm/850nm, 550m, Hardened -40~75°C
S35-2SLC-10	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 10km, Hardened -40~75°C
S35-2SLC-30	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1310nm/1310nm, 30km, Hardened -40~75°C
S35-2SLC-70	SFP, LC Connector, Single Mode, Gigabit, 2 fiber,1550nm/1550nm, 70km, Hardened -40~75°C

Fast Ethernet SFP Transceiver Modules**Error! Not a valid link.**

1. It is recommended to use IFS SFPs on the **Industrial Managed Switch**. If you insert an SFP transceiver that is not supported, the **Industrial Managed Switch** will not recognize it.
2. Please choose the SFP transceiver which is appropriate for the operating environment.

1000Base-SX/LX:

Before connecting the other switches, workstation or media converter.

1. Make sure both sides of the SFP transceiver are with the same media type, for example, 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.
2. Check the fiber-optic cable type that matches the SFP transceiver model.
   - To connect to 1000Base-SX SFP transceiver, use the multi-mode fiber cable with one side being the male duplex LC connector type.
   - To connect to 1000Base-LX SFP transceiver, use the single-mode fiber cable with one side being the male duplex LC connector type.

Connect the fiber cable

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a media converter.
3. Check the LNK/ACT LED of the SFP slot on the front of the **Industrial Managed Switch**. Ensure that the SFP transceiver is operating correctly.

100Base-FX:

Before connecting the other switches, workstation or media converter.

1. Make sure both sides of the SFP transceiver are with the same media type or WDM pair; for example, 100Base-FX to 100Base-FX, 100Base-BX20-U to 100Base-BX20-D.
2. Check the fiber-optic cable type that matches the SFP transceiver model.
   - To connect to MFB-FX SFP transceiver, use the multi-mode fiber cable with one side being the male duplex LC connector type.
   - To connect to MFB-F20/F40/F60/FA20/FB20 SFP transceiver, use the single-mode fiber cable with one side being the male duplex LC connector type.

Connect the fiber cable

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a media converter.

3. Check the LNK/ACT LED of the SFP slot of the switch/converter. Ensure that the SFP transceiver is operating correctly.

4. Check the Link mode of the SFP port if the link fails. Co works with some fiber-NICs or media converters. Set the Link mode to "**100 Force**" when needed.

2.3.2 Remove the Module

1. Make sure there is no network activity by checking with the network administrator, or through the management interface of the switch/converter (if available) to disable the port in advance.

2. Remove the Fiber Optic Cable gently.

3. Lift up the lever of the MGB/MFB module and turn it to a horizontal position.

4. Pull out the module gently through the lever.

Figure 2-10: How to Pull Out the SFP Transceiver Module

Note

Never pull out the module without lifting up the lever of the module and turning it to a horizontal position. Directly pulling out the module could damage the module and the SFP module slot of the Managed Switch.

3. SWITCH MANAGEMENT

This chapter explains the methods that you can use to configure management access to the **Industrial Managed Switch**. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Remote Telnet Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- Workstations of subscribers running Windows XP/2003, Vista, Windows 7, MAC OS X, Linux, Fedora, Ubuntu or other platform compatible with **TCP/IP** protocols.
- **The Workstation** is installed with **Ethernet NIC** (Network Interface Card)
- Ethernet Port connection
  - Network cables - Use standard network (UTP) cables with RJ45 connectors.
  - The above Workstation is installed with **WEB Browser** and **JAVA runtime environment** Plug-in

It is recommended to use Internet Explorer 7.0 or above to access **Industrial Managed Switch**.

3.2 Management Access Overview

The **Industrial Managed Switch** gives you the flexibility to access and manage it using any or all of the following methods:

- Remote Telnet Interface
- **Web browser** Interface
- An external **SNMP-based network management application**

The Remote Telnet and Web browser interface support are embedded in the **Industrial Managed Switch** software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Remote Telnet	• Text-based • Telnet functionality built into Windows XP/2003, Vista, Windows 7 operating systems • Can be accessed from any location	• Security can be compromised (hackers need only know the IP address)
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1: Management Methods Comparaison

3.3 CLI Mode Management

There are two ways for CLI mode management, one is remote telnet, and the other is operating from console port. Remote telnet is an IP-based protocol, and console port is for user to operate the Industrial Managed Switch on local only; however their operation is the same.

The command line user interface is for performing system administration, such as displaying statistics or changing option settings. Using this method, you can access the **Industrial Managed Switch** remote telnet interface from personal computer or workstation in the same Ethernet environment as long as you know the current IP address of the **Industrial Managed Switch**.

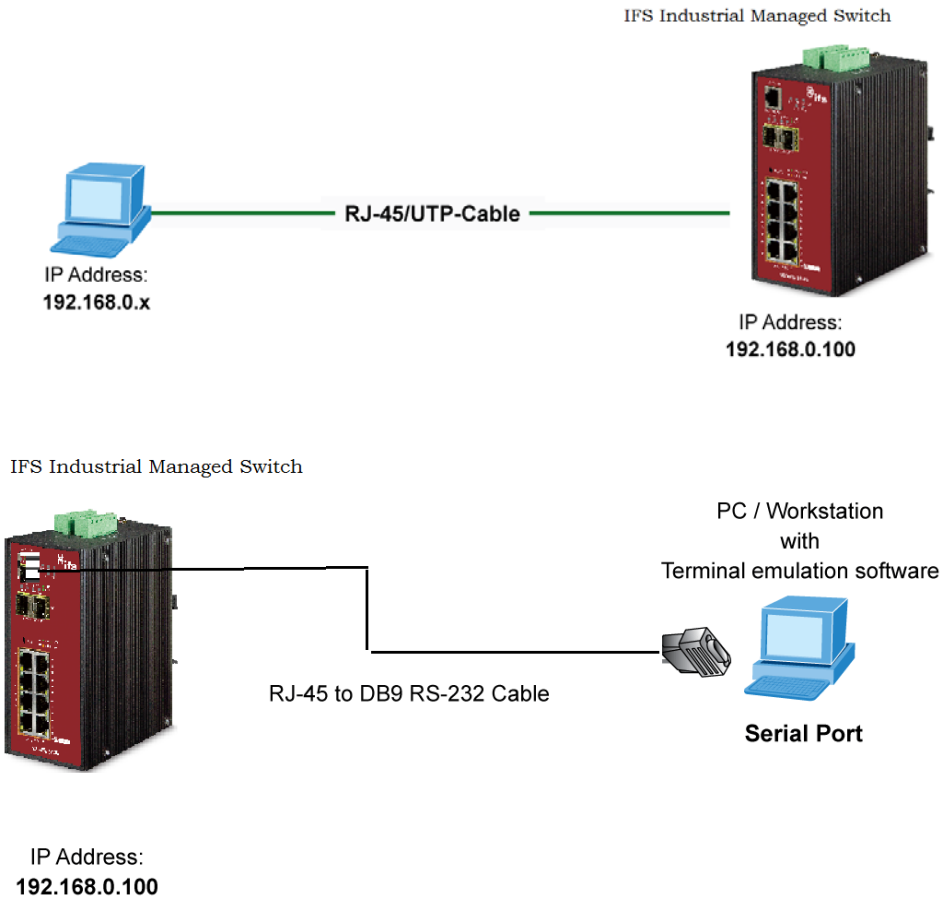


Figure 3-1: Remote Telnet and Console Port Interface Management

In Windows system, you may click **"Start"** and then choose **"Acessories"** and **"Command Prompt"**. Please input **"telnet 192.168.0.100"** and press **"enter'** from your keyboard. The following screen (see Figure 3-2) will appear.

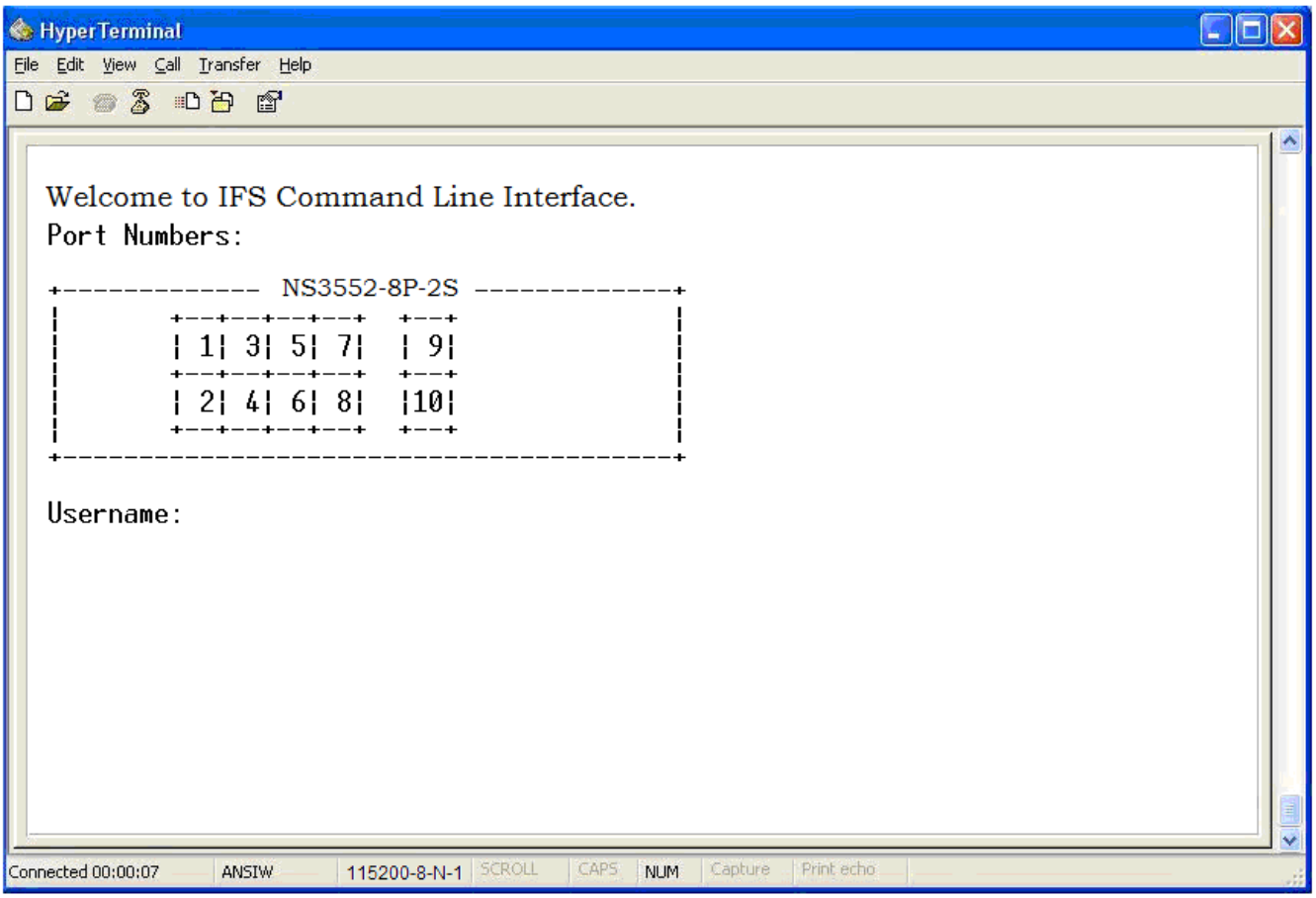


Figure 3-2: Remote Telnet Interface Main Screen of **Industrial Managed Switch**

For more information about using the Remote Telnet interface, refer to **Chapter 5 Remote Telnet Interface Management**.

3.4 Web Management

The **Industrial Managed Switch** offers management features that allow users to manage the **Industrial Managed Switch** from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After you set up your IP address for the **Industrial Managed Switch**, you can access the **Industrial Managed Switch**'s Web interface applications directly in your Web browser by entering the IP address of the **Industrial Managed Switch**.

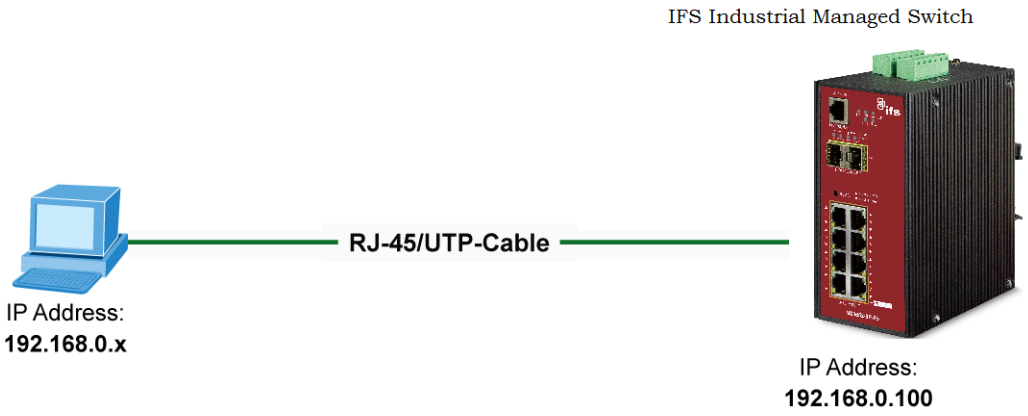


Figure 3-3: Web Management

You can then use your Web browser to list and manage the **Industrial Managed Switch** configuration parameters from one central location; the Web Management requires **Microsoft Internet Explorer 7.0** or later.

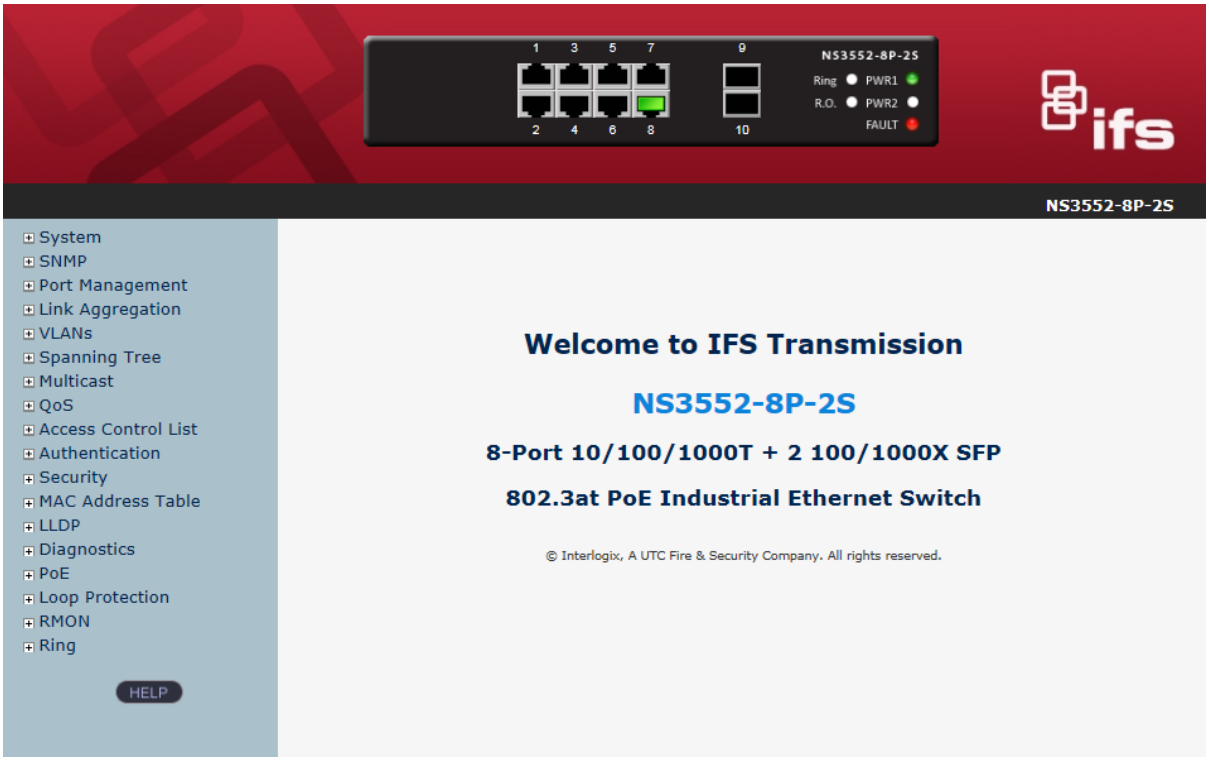


Figure 3-4: Web Main Screen of **Industrial Managed Switch**

3.5 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the **Industrial Managed Switch**, such as SNMP Network Manager, HP Open view Network Node Management (NNM) or What's Up Gold. This management method requires the SNMP agent on the Industrial **Managed Switch** and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP Net-work management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default getting and setting community strings for the **Industrial Managed Switch** are public.

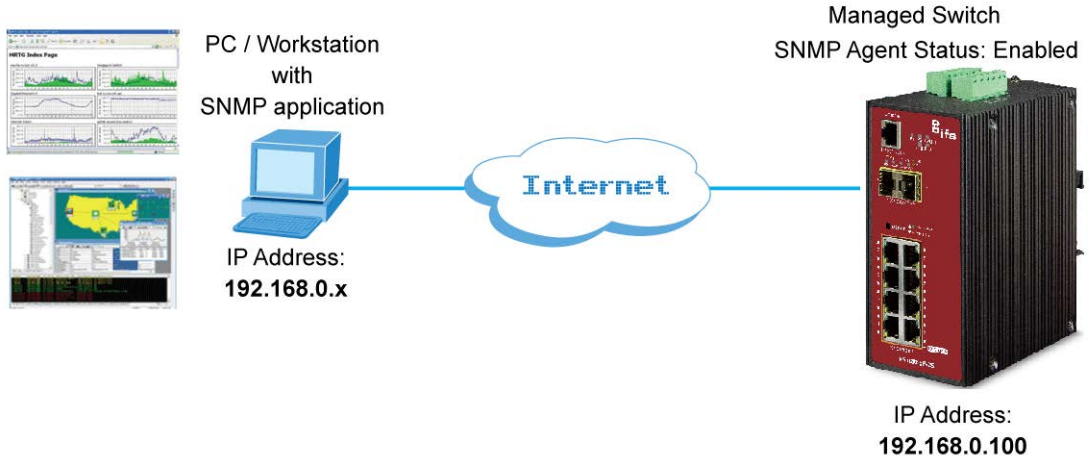


Figure 3-5: SNMP Management

4. WEB CONFIGURATION

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

The **Industrial Managed Switch** offers management features that allow users to manage the **Industrial Managed Switch** from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-based Management supports Internet Explorer 7.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

By default, IE7.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The **Industrial Managed Switch** can be configured through an Ethernet connection, making sure the manager PC must be set on the same IP subnet address as the **Industrial Managed Switch**.

For example, the default IP address of the **Industrial Managed Switch** is ***192.168.0.100***, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the **Industrial Managed Switch** to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.

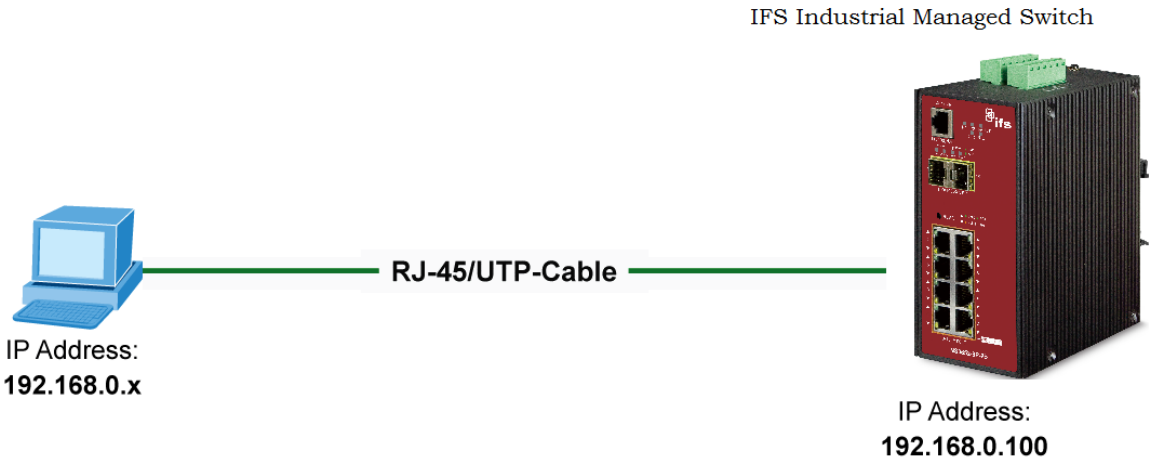


Figure 4-1-1: Web Management

- **Gentlogging on the Industrial Managed Switch**

1. Use Internet Explorer 7.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The

factory-default IP Address is shown as follows:

http://192.168.0.100

2. When the following login screen appears, please enter the default username "**admin**" with password "**admin**" (or the username/password you have changed via console) to login the main screen of **Industrial Managed Switch**. The login screen in Figure 4-1-2 appears.

Connect to 192.168.0.100
The server 192.168.0.100 at Web Management requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

Figure 4-1-2: Login Screen

Default User name: **admin**

Default Password: **admin**

After entering the username and password, the main screen appears as Figure 4-1-3.

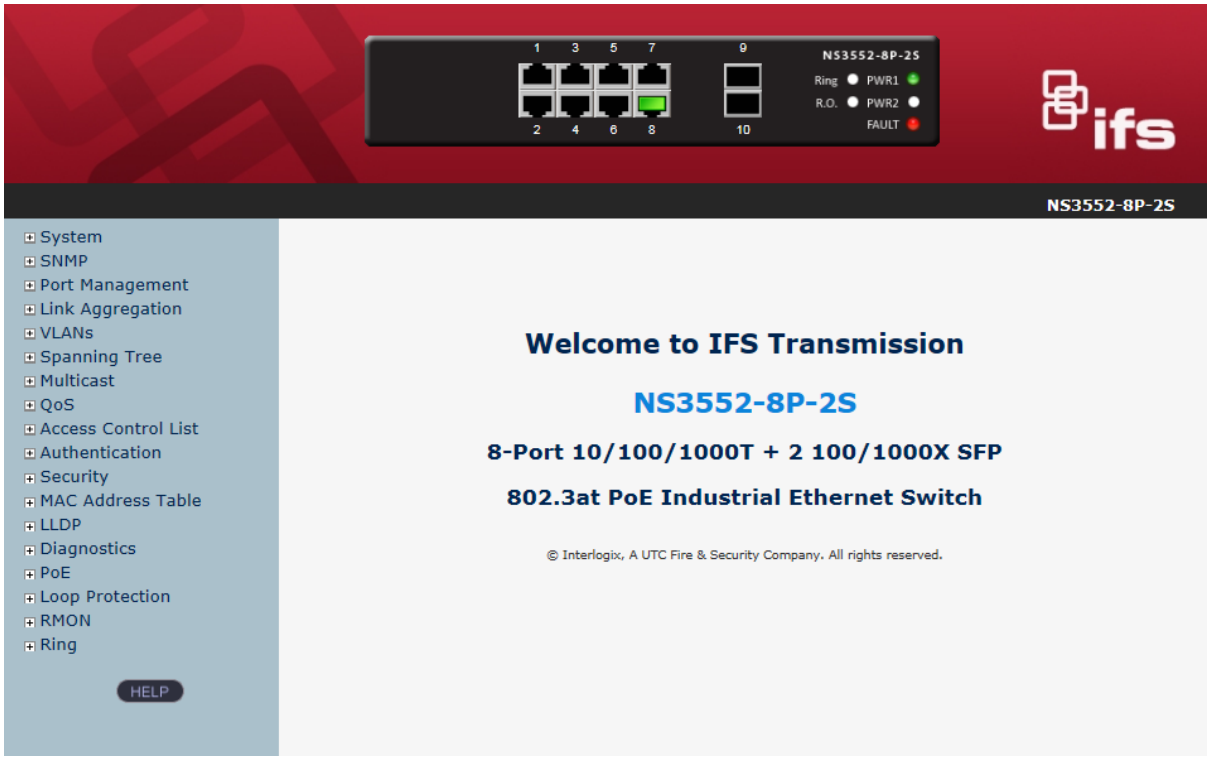


Figure 4-1-3: Default Main Page

Now, you can use the Web management interface to continue the switch management or manage the **Industrial Managed Switch** by Web interface. The Switch Menu on the left of the web page lets you access all the commands and statistics the Managed Switch provides.

Note

1. It is recommended to use Internet Explorer 7.0 or above to access **Industrial Managed Switch**.
2. The changed IP address takes effect immediately after clicking on the **Save** button. You need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.
4. Only accept command in lowercase letter under web interface.

4.1 Main Web Page

The **Industrial Managed Switch** provides a Web-based browser interface for configuring and managing it. This interface allows you to access the **Industrial Managed Switch** using the Web browser of your choice. This chapter describes how to use the **Industrial Managed Switch**'s Web browser interface to configure and manage it.

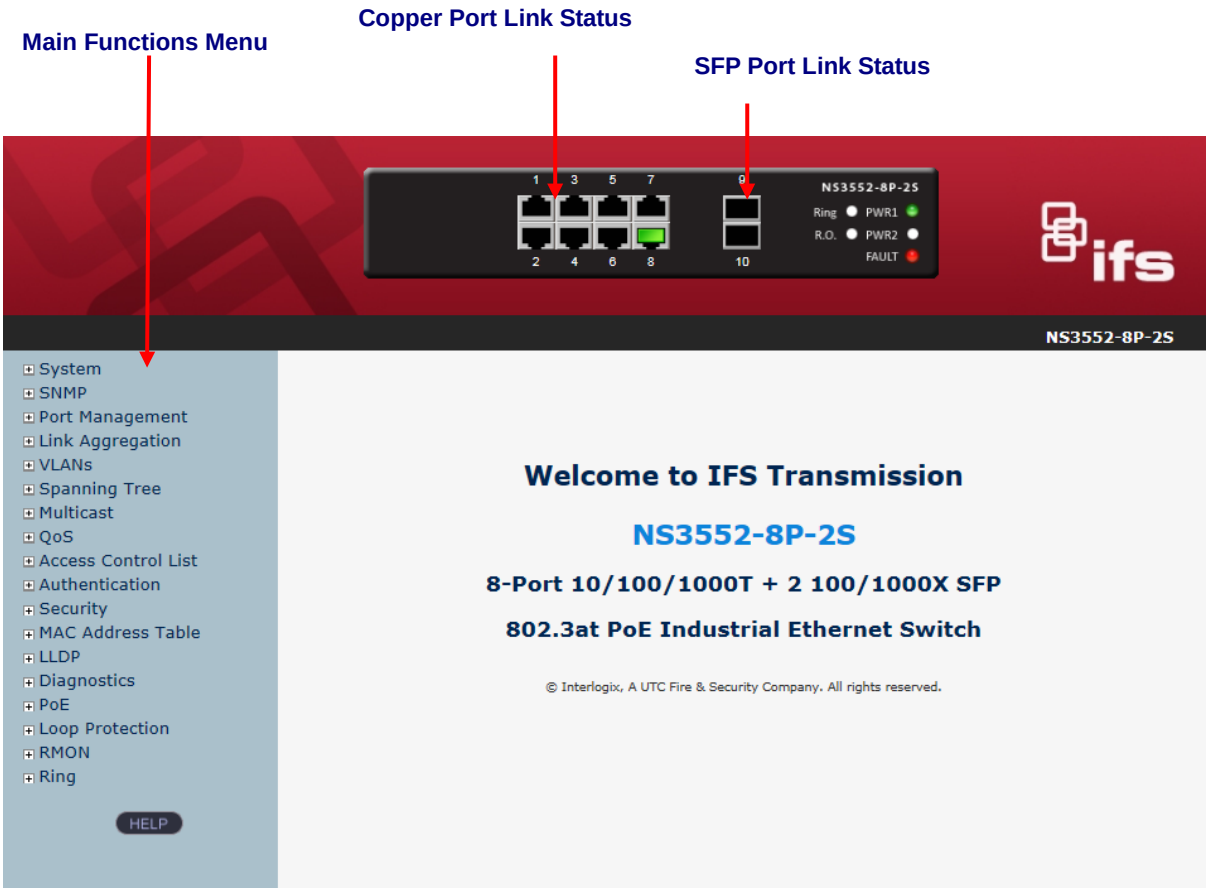


Figure 4-1-4: Main Page

Panel Display

The web agent displays an image of the **Industrial Managed Switch**'s ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the **Port Statistics** page. The port states are illustrated as follows:

State	Disabled	Link Down	Link Up	PoE On
RJ-45 Ports				
SFP Ports				Not Supported

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the **Industrial Managed Switch**, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the **Industrial Managed Switch** by selecting the functions those listed in the Main Function. The screen in Figure 4-1-5 appears.

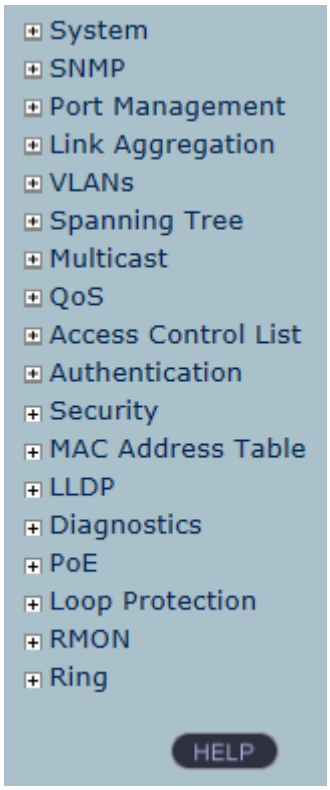


Figure 4-1-5: Industrial Managed Switch Main Functions Menu

4.2 System

Use the System menu items to display and configure basic administrative details of the **Industrial Managed Switch**. Under the System the following topics are provided to configure and view the system information.

4.2.1 System Information

The System Info page provides information for the current device information. System Info page helps a switch administrator to identify the hardware MAC address, software version and system uptime. The screen in Figure 4-2-1 appears.

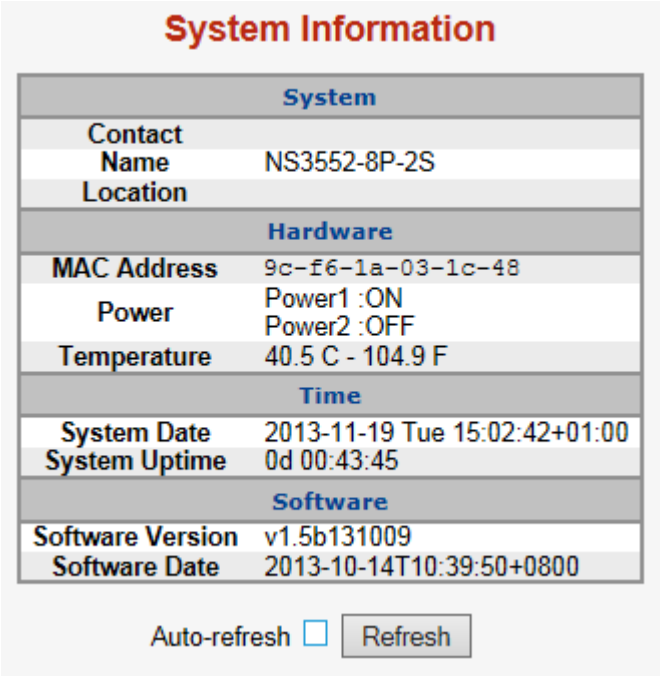


Figure 4-2-1: System Information Page Screenshot

The page includes the following fields:

Object	Description
• **Contact**	The system contact configured in Configuration | System | Information | System Contact.
• **Name**	The system name configured in Configuration | System | Information | System Name.
• **Location**	The system location configured in Configuration | System | Information | System Location.
• **MAC Address**	The MAC Address of this **Industrial Managed Switch**.
• **Power**	The Power 1 and Power 2 ON/OFF Status display.
• **Temperature**	The Temperature shows current of the switch inside temperature status.
• **System Date**	The current (GMT) system time and date. The system time is obtained through the configured SNTP Server, if any.
• **System Uptime**	The period of time the device has been operational.
• **Software Version**	The software version of the **Industrial Managed Switch**.
• **Software Date**	The date when the switch software was produced.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

4.2.2 IP Configuration

The IP Configuration includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration. Fill out the IP Address, Subnet Mask and Gateway for the device. The screen in Figure 4-2-2 appears.

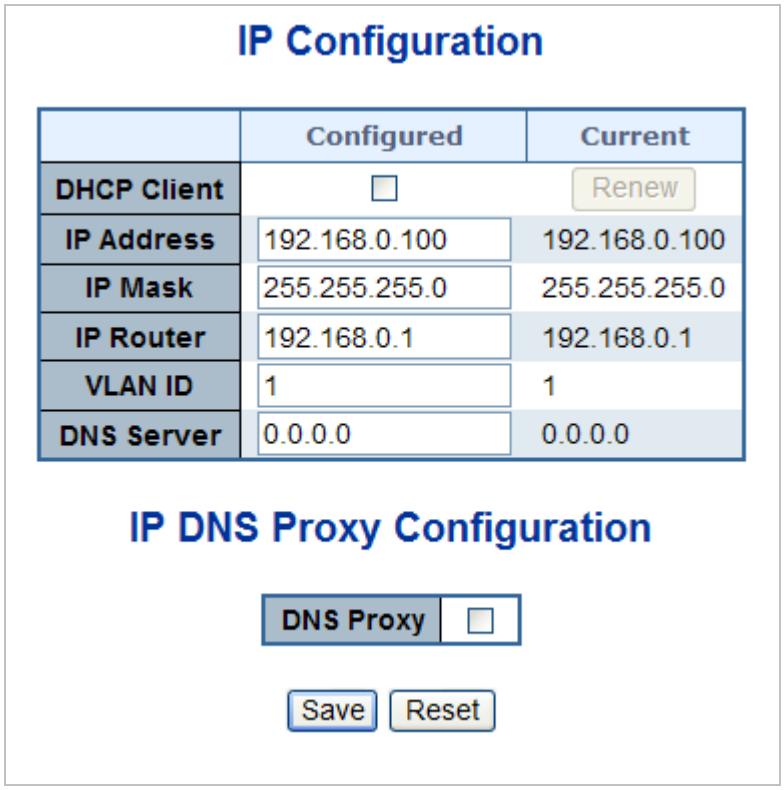


Figure 4-2-2: IP Configuration Page Screenshot

The Current column is used to show the active IP configuration.

Object	Description
• **DHCP Client**	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP server does not respond around 35 seconds and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as host name to provide DNS lookup.
• **IP Address**	Provide the IP address of this switch in dotted decimal notation.
• **IP Mask**	Provide the IP mask of this switch dotted decimal notation.
• **IP Router**	Provide the IP address of the router in dotted decimal notation.
• **VLAN ID**	Provide the managed VLAN ID. The allowed range is **1** through **4095**.
• **DNS Server**	Provide the IP address of the DNS Server in dotted decimal notation.
• **DNS Proxy**	When DNS proxy is enabled, DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client device on the network.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Renew: Click to renew DHCP Client. This button is only available if DHCP Client is enabled.

4.2.3 IPv6 Configuration

Configure the switch-managed IPv6 information on this page.

The Configured column is used to view or change the IPv6 configuration. The Current column is used to show the active IPv6 configuration. The screen in Figure 4-2-3 appears.

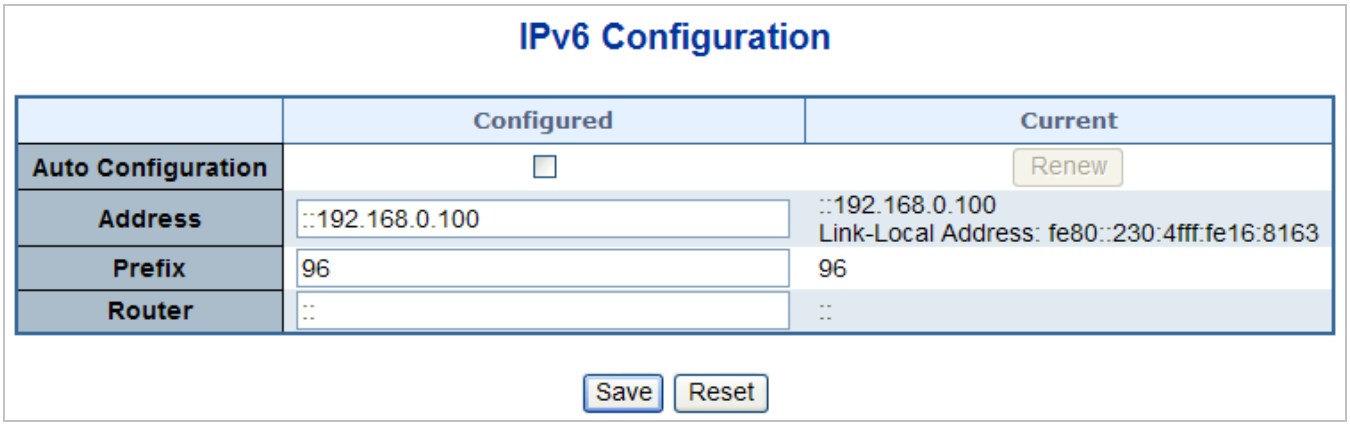


Figure 4-2-3: IPv6 Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Auto Configuration**	Enable IPv6 auto-configuration by checking this box. If system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds. The total time needed to complete auto-configuration can be significantly longer.
• **Address**	Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
• **Prefix**	Provide the IPv6 Prefix of this switch. The allowed range is **1** to **128**.
• **Router**	Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. . For example, '192.1.2.34'.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Renew: Click to renew IPv6 Auto Configuration. This button is only available if IPv6 Auto Configuration is enabled.

4.2.4 Users Configuration

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser. After setup is completed, please press **"Save"** button to take effect. Please login web interface with new user name and password, the screen in Figure 4-2-4 appears.

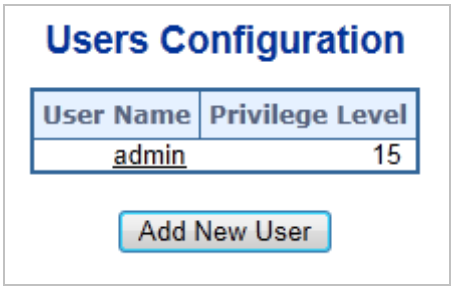


Figure 4-2-4: Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	The name identifies the user.
• **Privilege Level**	The privilege level of the user. The allowed range is **1** to **15**. If the privilege level value is 15, it can access all groups i.e. that is granted the full control of the device. But others value need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have the access to that group. By default setting, almost group privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults, etc.) needs user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Add New User: Click to add a new user.

Add / Edit User

This page configures a user – add, edit or delete user.

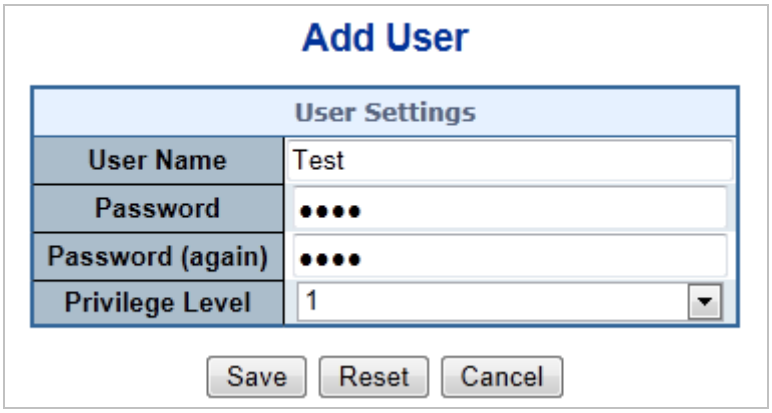


Figure 4-2-5: Add / Edit User Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	A string identifies the user name whose entry should belong to. The allowed string length is **1** to **32**. The valid user name is a combination of letters, numbers and underscores.
• **Password**	The password of the user. The allowed string length is **0** to **32**.
• **Privilege Level**	The privilege level of the user. The allowed range is **1** to **15**. If the privilege level value is 15, it can access all groups, i.e. which is granted the full control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access to that group. By default setting, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the Users.

Delete User: Delete the current user. This button is not available for new configurations (Add new user)

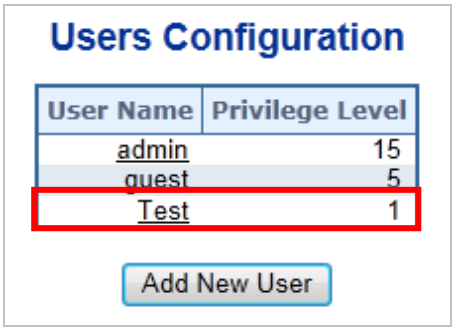
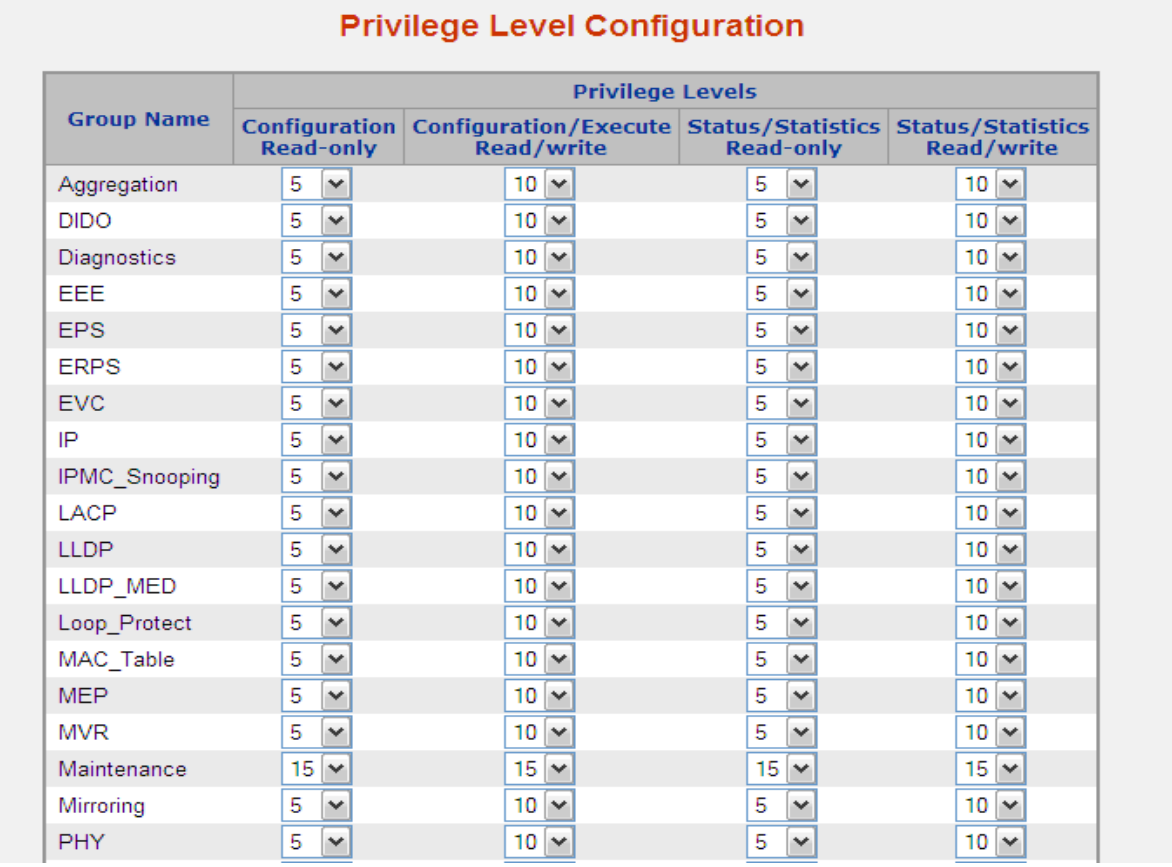


Figure 4-2-6: User Configuration Page Screenshot

After changing the default password, if you forget the password, please press the ***"Reset"*** button on the front panel of the **Industrial Managed Switch** over 10 seconds and then release. The current setting includes VLAN, and will be lost and the **Industrial Managed Switch** will restore to the default mode.

4.2.5 Privilege Levels

This page provides an overview of the privilege levels. After setup is completed, please press **"Save"** button to take effect. Please login web interface with new user name and password, the screen in Figure 4-2-7 appears.



Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
DIDO	5	10	5	10
Diagnostics	5	10	5	10
EEE	5	10	5	10
EPS	5	10	5	10
ERPS	5	10	5	10
EVC	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
LLDP_MED	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MEP	5	10	5	10
MVR	5	10	5	10
Maintenance	15	15	15	15
Mirroring	5	10	5	10
PHY	5	10	5	10

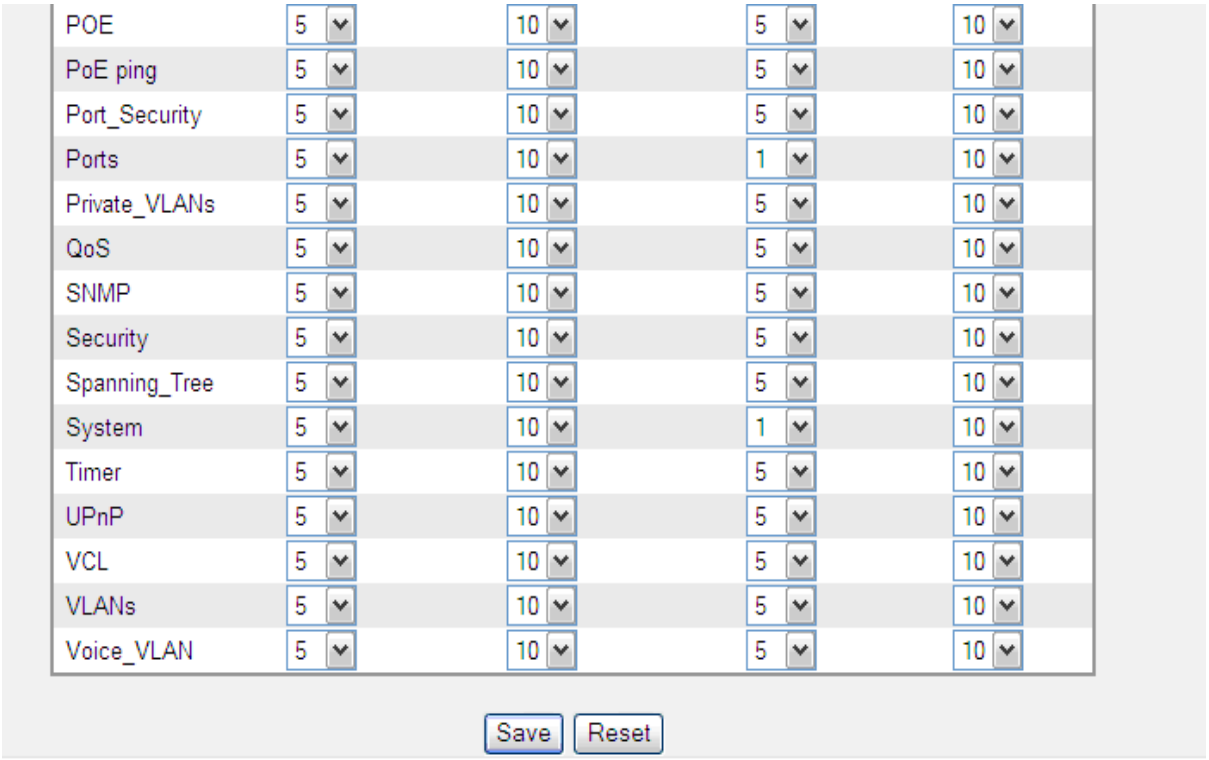

POE 5 10 5 10
PoE ping 5 10 5 10
Port_Security 5 10 5 10
Ports 5 10 1 10
Private_VLANs 5 10 5 10
QoS 5 10 5 10
SNMP 5 10 5 10
Security 5 10 5 10
Spanning_Tree 5 10 5 10
System 5 10 1 10
Timer 5 10 5 10
UPnP 5 10 5 10
VCL 5 10 5 10
VLANs 5 10 5 10
Voice_VLAN 5 10 5 10
Save
Reset

Figure 4-2-7: Privilege Levels Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Group Name**	The name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details: ■ **System**: Contact, Name, Location, Time zone, Log. ■ **Security**: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard. ■ **IP**: Everything except 'ping'. ■ **Port**: Everything except 'VeriPHY'. ■ **Diagnostics**: 'ping' and 'VeriPHY'. ■ **Maintenance**: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web-Users, Privilege Levels and everything in Maintenance. ■ **Debug**: Only present in CLI.
• **Privilege Level**	Every group has an authorization Privilege level for the following sub groups: ■ **Configuration read-only** ■ **Configuration/execute read-write** ■ **Status/statistics read-only** ■ **Status/statistics read-write** (e.g. for clearing of statistics). User Privilege should be the same or greater than the authorization Privilege level to have the access to that group.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.6 NTP Configuration

Configuring NTP on this page.

NTP is an acronym for **Network Time Protocol**, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (data grams) as transport layer. You can specify NTP Servers and set GMT Time zone. The NTP Configuration screen in Figure 4-2-8 appears.

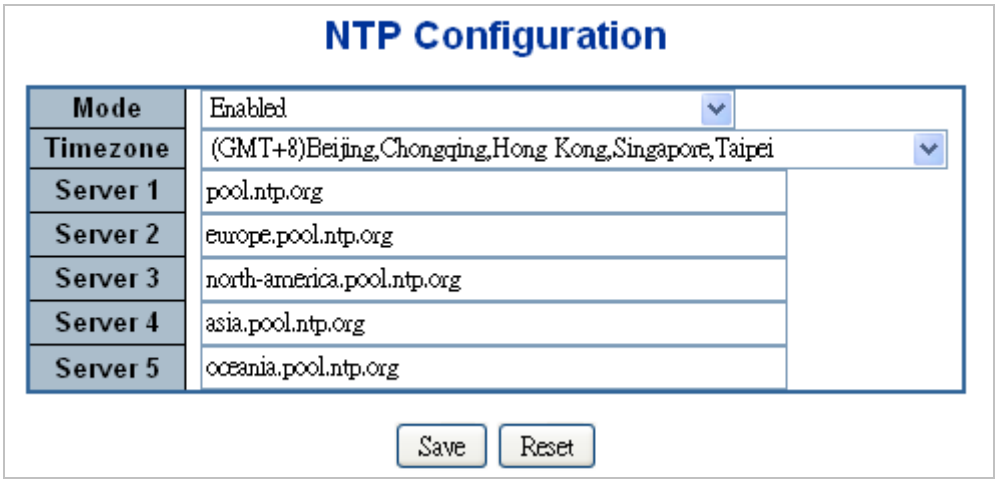


Figure 4-2-8: NTP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the NTP mode operation. Possible modes are: ■ **Enabled**: Enable NTP mode operation. When NTP mode operation is enabled, the agent forwards NTP messages between the clients and the server when they are not on the same subnet domain. ■ **Disabled**: Disable NTP mode operation.
• **Time zone**	Allows to select the time zone according to current location of switch.
• **Server #**	Provides the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '192.1.2.34'.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.7 Daylight Saving

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user will re-access the WEB interface about 60 seconds later. The System Reboot screen in Figure 4-2-9 appears.

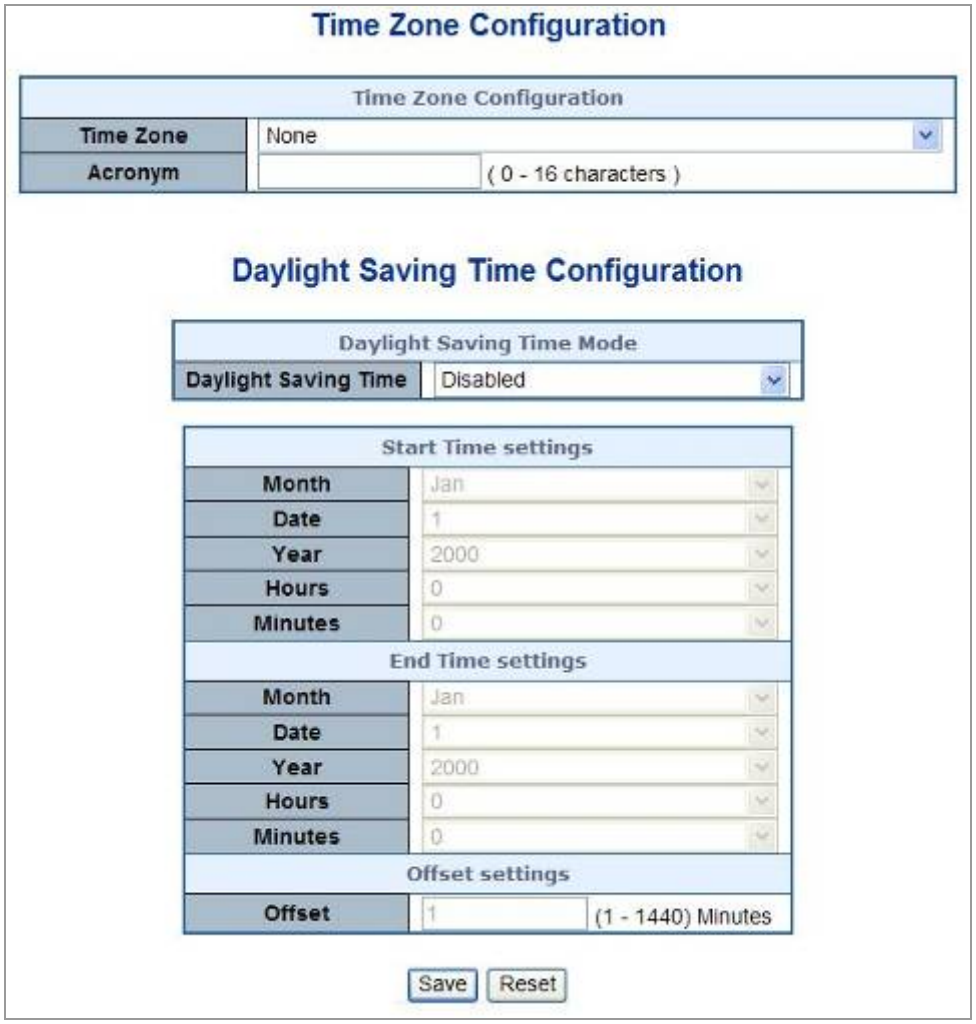


Figure 4-2-9: System Reboot Page Screenshot

The page includes the following fields:

Object	Description
• **Time Zone**	Allows to select the time zone according to current location of switch.
• **Acronym**	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 alpha-numeric characters and can contain '-', '_' or '.')
• **Daylight Saving Time**	It is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)

Daylight Saving Time – **Recurring Mode**

Object	Description
• **Week (Start Time Setting)**	Select the starting week number.
• **Day (Start Time Setting)**	Select the starting day.
• **Month (Start Time Setting)**	Select the starting month.
• **Hours (Start Time Setting)**	Select the starting hour.

• **Minutes (Start Time Setting)**	Select the starting minute.
• **Week (End Time Setting)**	Select the ending week number.
• **Day (End Time Setting)**	Select the ending day.
• **Month (End Time Setting)**	Select the ending month.
• **Hours (End Time Setting)**	Select the ending hour.
• **Month (End Time Setting)**	Select the ending minute.
• **Offset**	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Daylight Saving Time – **Non-Recurring Mode**

Object	Description
• **Month (Start Time Setting)**	Select the starting month.
• **Date (Start Time Setting)**	Select the starting date.
• **Year (Start Time Setting)**	Select the starting year.
• **Hours (Start Time Setting)**	Select the starting hour.
• **Minutes (Start Time Setting)**	Select the starting minute.
• **Month (End Time Setting)**	Select the ending month.
• **Date (End Time Setting)**	Select the ending date.
• **Year (End Time Setting)**	Select the ending year.
• **Hours (End Time Setting)**	Select the ending hour.
• **Minutes (End Time Setting)**	Select the ending minute.
• **Offset**	• Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.8 UPnP

Configuring UPnP on this page.

UPnP is an acronym for **Universal Plug and Play**. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. The UPnP Configuration screen in Figure 4-2-10 appears.

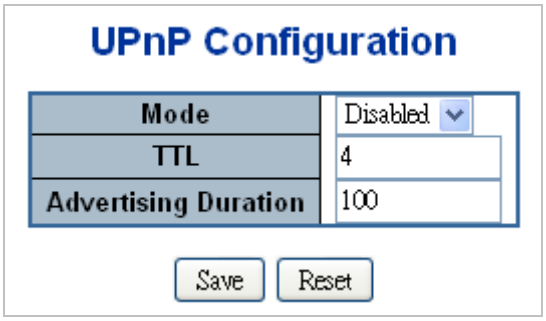


Figure 4-2-10: UPnP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the UPnP operation mode. Possible modes are: ■ **Enabled**: Enable UPnP mode operation. ■ **Disabled**: Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.
• **TTL**	The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range from 1 to 255.
• **Advertising Duration**	The duration, carried in SSDP packets, is used to inform a control point or control points about how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it may suggest that the switch no longer exists. Due to the unreliable nature of UDP, as standard it is recommended that such refreshment of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range from 100 to 86400.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

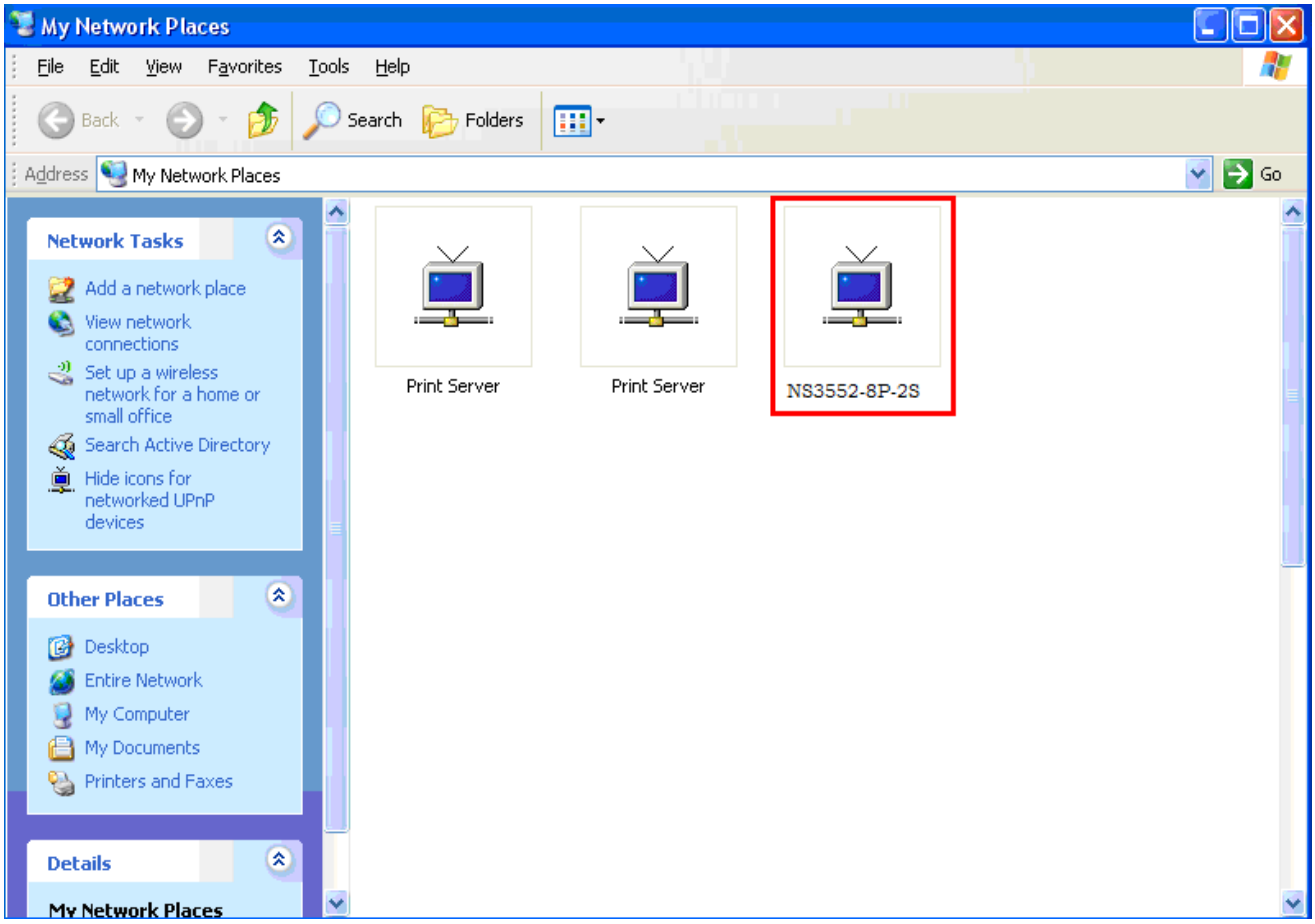


Figure 4-2-11: UPnP Devices shows on Windows My Network Places

4.2.9 DHCP Relay

Configuring DHCP Relay on this page

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The **DHCP option 82** enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options:

- Circuit ID (option 1)
- Remote ID (option2).

The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on.
The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes representing the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equals 0; in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal to the DHCP relay agent's MAC address. The DHCP Relay Configuration screen in Figure 4-2-12 appears.

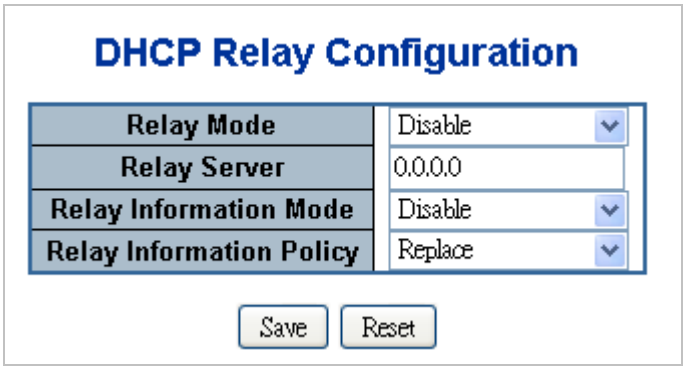


Figure 4-2-12: DHCP Relay Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Relay Mode**	Indicates the DHCP relay mode operation. Possible modes are: ■ **Enabled**: Enable DHCP relay mode operation. When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered. ■ **Disabled**: Disable DHCP relay mode operation.
• **Relay Server**	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when

	they are not on the same subnet domain.
• **Relay Information Mode**	Indicates the DHCP relay information mode option operation. Possible modes are: ■ **Enabled**: Enable DHCP relay information mode operation. When enable DHCP relay information mode operation, the agent insert specific information (option82) into a DHCP message when forwarding to DHCP server and remove it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled. ■ **Disabled**: Disable DHCP relay information mode operation.
• **Relay Information Policy**	Indicates the DHCP relay information option policy. When enable DHCP relay information mode operation, if agent receive a DHCP message that already contains relay agent information. It will enforce the policy. And it only works under DHCP relay information operation mode enabled. Possible policies are: ■ **Replace**: Replace the original relay information when receive a DHCP message that already contains it. ■ **Keep**: Keep the original relay information when receive a DHCP message that already contains it. ■ **Drop**: Drop the package when receive a DHCP message that already contains relay information.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.10 DHCP Relay Statistics

This page provides statistics for DHCP relay. The DHCP Relay Statistics screen in Figure 4-2-13 appears.

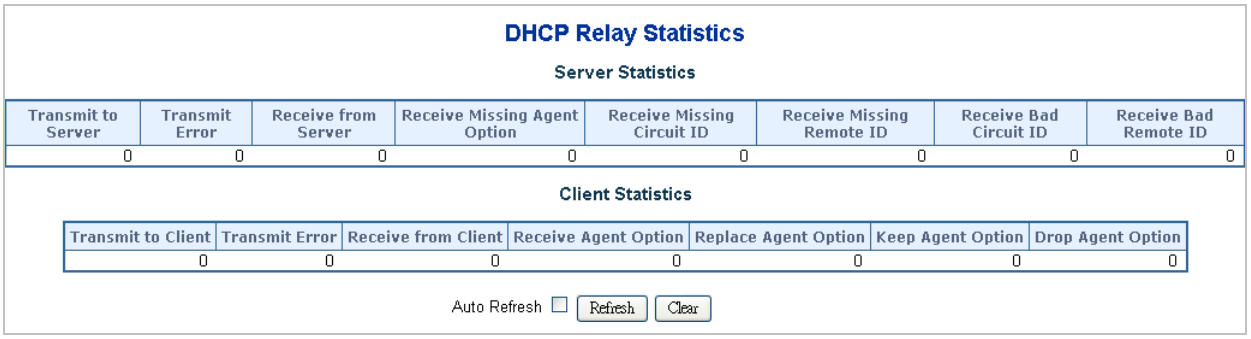


Figure 4-2-13: DHCP Relay Statistics Page Screenshot

The page includes the following fields:

Server Statistics

Object	Description
• **Transmit to Server**	The number of packets that are relayed from client to server.
• **Transmit Error**	The number of packets that resulted in errors while being sent to clients.
• **Receive form Server**	The number of packets received from server.

• **Receive Missing Agent Option**	The number of packets received without agent information options.
• **Receive Missing Circuit ID**	The number of packets received with the Circuit ID option missing.
• **Receive Missing Remote ID**	The number of packets received with the Remote ID option missing.
• **Receive Bad Circuit ID**	The number of packets whose Circuit ID option did not match known circuit ID.
• **Receive Bad Remote ID**	The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Object	Description
• **Transmit to Client**	The number of relayed packets from server to client.
• **Transmit Error**	The number of packets that resulted in error while being sent to servers.
• **Receive from Client**	The number of received packets from server.
• **Receive Agent Option**	The number of received packets with relay agent information option.
• **Replace Agent Option**	The number of packets which were replaced with relay agent information option.
• **Keep Agent Option**	The number of packets whose relay agent information was retained.
• **Drop Agent Option**	The number of packets that were dropped was received with relay agent information.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

4.2.11 CPU Load

This page displays the CPU load, using a **SVG graph**. The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG. The CPU Load screen in Figure 4-2-14 appears.

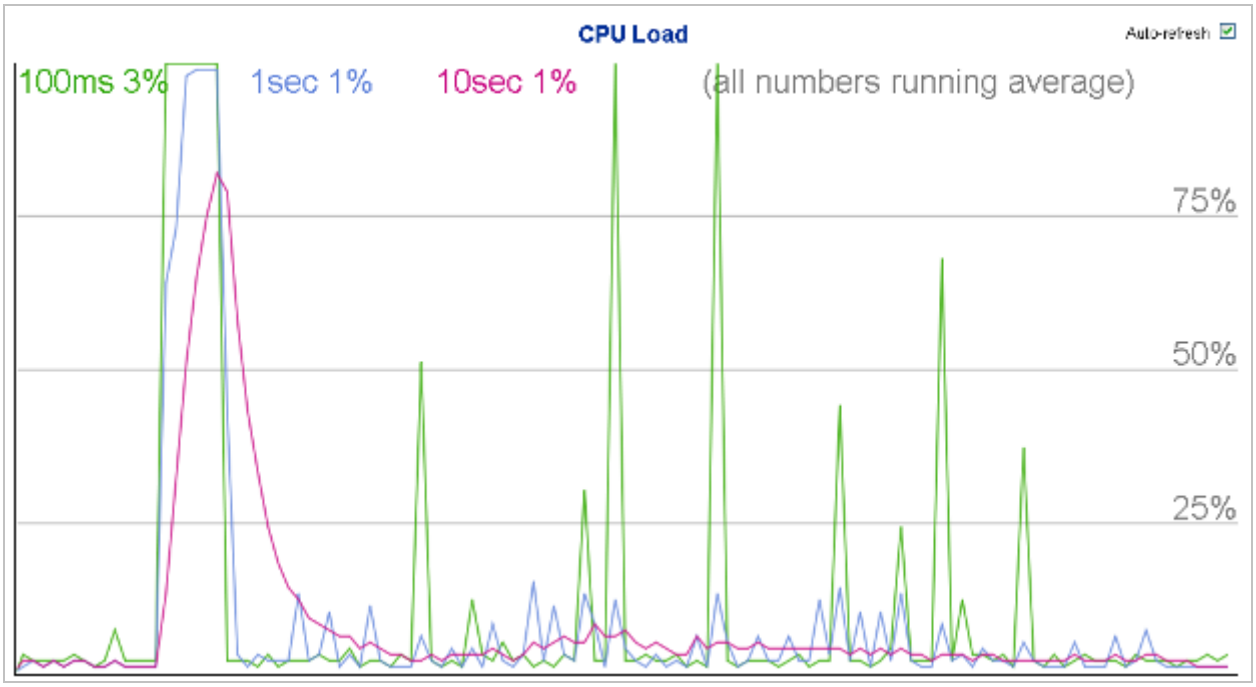


Figure 4-2-14: CPU Load Page Screenshot

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Note

If your browser cannot display anything on this page, please download Adobe SVG tool and install it in your computer.

4.2.12 System Log

The switch system log information is provided here. The System Log screen in Figure 4-2-15 appears.

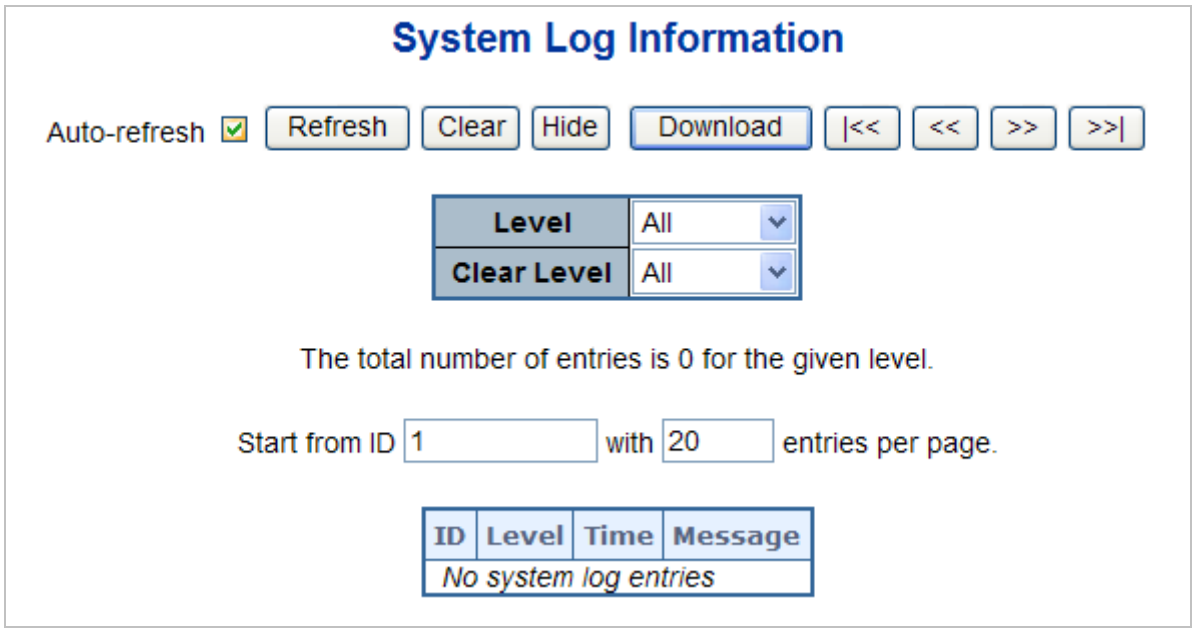


Figure 4-2-15: System Log Page Screenshot

The page includes the following fields:

Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Level**	The level of the system log entry. The following level types are supported: ■ **Info**: Information level of the system log. ■ **Warning**: Warning level of the system log. ■ **Error**: Error level of the system log. ■ **All**: All levels.
• **Time**	The time of the system log entry.
• **Message**	The message of the system log entry.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to update the system log entries, starting from the current entry ID

Clear: Flushes the selected log entries.

Hide: Hide system log according to entry page. As default System Log Information shows 20 entries for one page. Hide button can hide the system log entry that has been over one page.

Download: Click this button to download system log with CSV format file.

|<<: Updates the system log entries, starting from the first available entry ID.

<<: Updates the system log entries, ending at the last entry currently displayed.

>>: Updates the system log entries, starting from the last entry currently displayed.

>>|: Updates the system log entries, ending at the last available entry ID.

4.2.13 Detailed Log

The switch system detailed log information is provided here. The Detailed Log screen in Figure 4-2-16 appears.

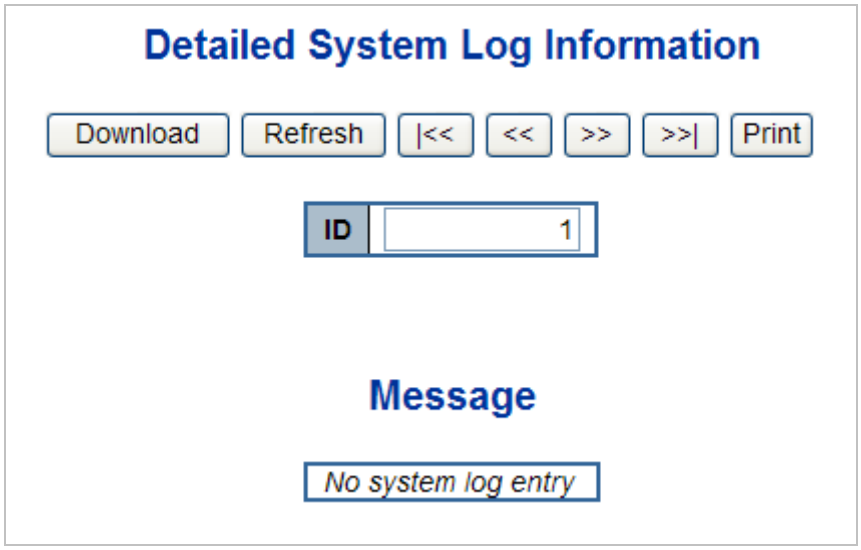


Figure 4-2-16: Detailed Log Page Screenshot

The page includes the following fields:

Object	Description
• **ID**	The ID (>= 1) of the system log entry.
• **Message**	The message of the system log entry.

Buttons

Download: Click this button to download system log with CSV format file.

Refresh: Updates the system log entry to the current entry ID.

|<<: Updates the system log entry to the first available entry ID

<<: Updates the system log entry to the previous available entry ID.

>>: Updates the system log entry to the next available entry ID.

>>|: Updates the system log entry to the last available entry ID.

Print: Click this button to print out system log.

4.2.14 Remote Syslog

Configure remote syslog on this page. The Remote Syslog screen in Figure 4-2-17 appears.

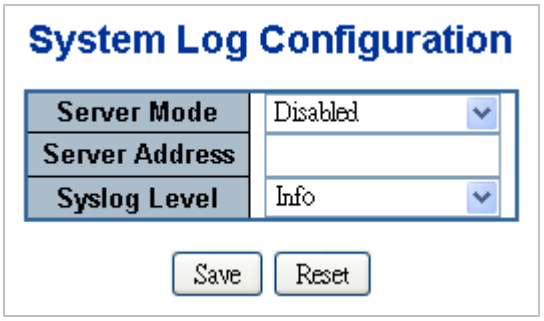


Figure 4-2-17: Remote Syslog Page Screenshot

The page includes the following fields:

Object	Description
• **Server Mode**	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: ■ **Enabled**: Enable server mode operation. ■ **Disabled**: Disable server mode operation.
• **Server Address**	Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.
• **Syslog Level**	Indicates what kind of message will send to syslog server. Possible modes are: ■ **Info**: Send information, warnings and errors. ■ **Warning**: Send warnings and errors. ■ **Error**: Send errors.

Buttons

Save: Click to save changes.

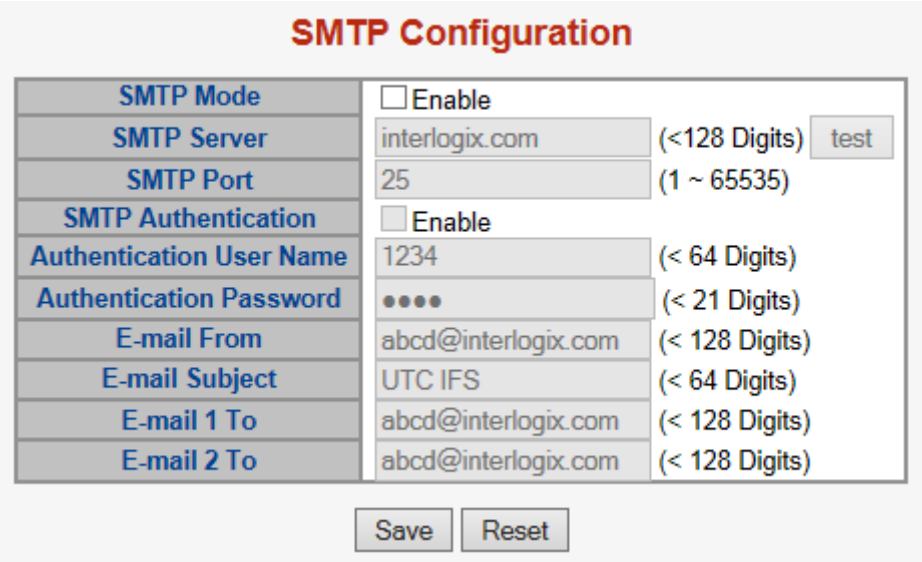
Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.15 SMTP Configuration

Configuring SMTP Configuration on this page

The SMTP Configuration screen in Figure 4-2-18 appears.

Figure 4-2-18: SMTP Configuration



The page includes the following fields:

Object	Description
• **SMTP Mode**	**Enabled** It is for you to enable SMTP mode function. This mode offers you to configure SMTP server and SMTP account information, system will refer it to send an E-mail for alarm noticing
• **SMTP Server**	It is for you to set up a specified SMTP server DNS name or IP address. If a DNS name is inputted; please remember to input DNS server IP address on the IP configuration page.
• **SMTP Port**	It is for you to input the SMTP server port number. The default is "25".
• **SMTP Authentication**	**Enabled** As usual SMTP server is denied to relay a mail from a different domain, so you have to enable this option and input your mail account and password for SMTP sever authorizing to forward a mail from a different domain. For example, you want an SMTP server, which is located on mail.**123.com**, to send a mail to mail.**456.net.com**. If you want to send the mail to a SMTP server which is located on the same domain or the same SMTP server, you don't have to enable SMTP authentication.
• **Authentic User Name**	It is for you to input your mail account name.
• **Authentication Password**	It is for you to input your mail account password.
• **E-mail From**	It is for you to input who send this mail.
• **E-mail Subject**	It is for you to input mail subject.

• **E-mail 1 To**	It is for you to input recipient mail address.
• **E-mail 2 To**	It is for you to input secondary recipient mail address.

Buttons

test: Click to test SMTP server address.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.16 Digital Input/output

Digital Input allows user to log external device (such as industrial cooler) dead or alive or something else. System will log a user customized message into system log and syslog, and issue SNMP trap or issue an alarm E-mail.

Digital Output allows user to monitor the switch port and power, and let system issue a high or low signal to an external device (such as alarm) when the monitor port or power has been failed. The Configuration screen in Figure 4-2-19 appears.

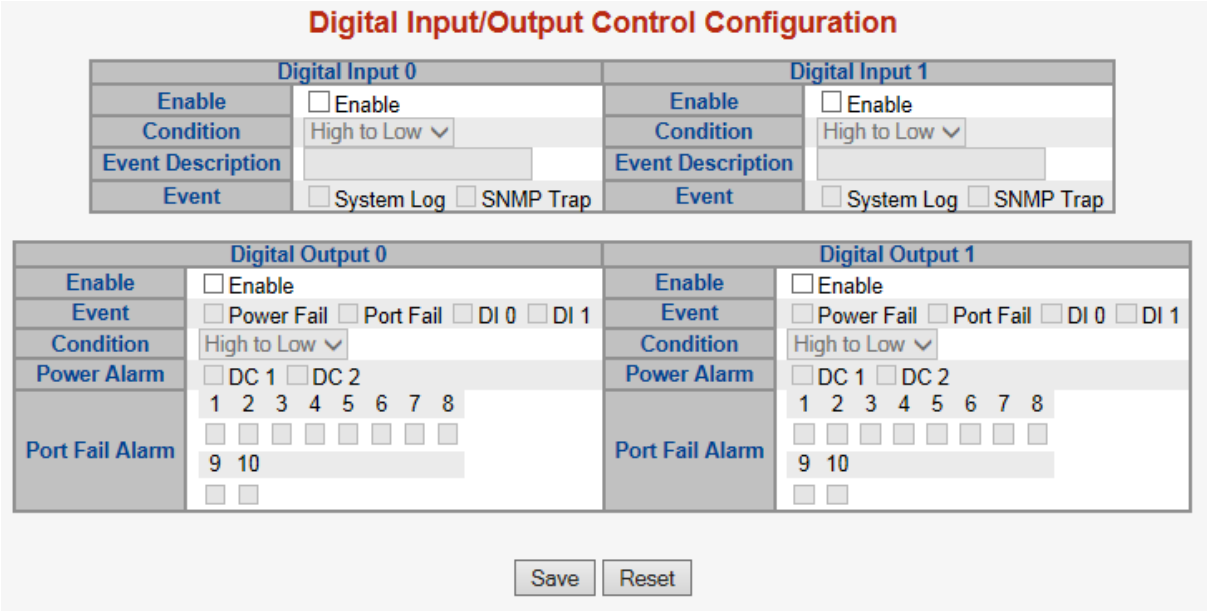


Figure 4-2-19 Windows File Selection Menu Popup

The page includes the following fields:

Object	Description
• **Enable**	Check the Enable checkbox to enable Digital Input / output function. Uncheck the Enable checkbox to disable Digital input / output function.

• **Condition**	**As Digital Input:** Allows user to select High to Low or Low to High. This means a signal received by system is from High to Low or From Low to High. It will trigger an action that logs a customize message or issue the message from the switch. **As Digital Output:** Allows user to select High to Low or Low to High. This means that when the switch is power-failed or port-failed, then system will issue a High or Low signal to an external device such as an alarm.
• **Event Description**	Allows user to set a customized message for Digital Input function alarming.
• **Event**	**As Digital Input:** Allows user to record alarm message to System log, syslog or issues out via SNMP Trap or SMTP. As default SNMP Trap and SMTP are disabled, please enable them first if you want to issue alarm message via them. **As Digital Output:** Allows user to monitor an alarm from port failure, power failure, Digital Input 0 (DI 0) and Digital Input 1(DI 1) which means if Digital Output has detected these events, then Digital Output would be triggered according to the setting of Condition.
• **Power Alarm**	Allows user to choose which power module that needs to be monitored.
• **Port Alarm**	Allows user to choose which port that needs to be monitored.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.17 Fault Alarm

The Fault Relay Alarm function provides the Power Failure and Port Link Down/Broken detection. With both power input 1 and power input 2 installed and the check boxes of power 1/power 2 ticked, the FAULT LED indicator will then be possible to light up when any one of the power failures occurs. As for the Port Link Down/Broken detection, the FAULT LED indicator will light up when the port failure occurs; certainly the check box beside the port must be ticked first. Please refer to the segment of '**Wiring the Fault Alarm Contact**' for the failure detection. The Configuration screen in Figure 4-2-20 appears.

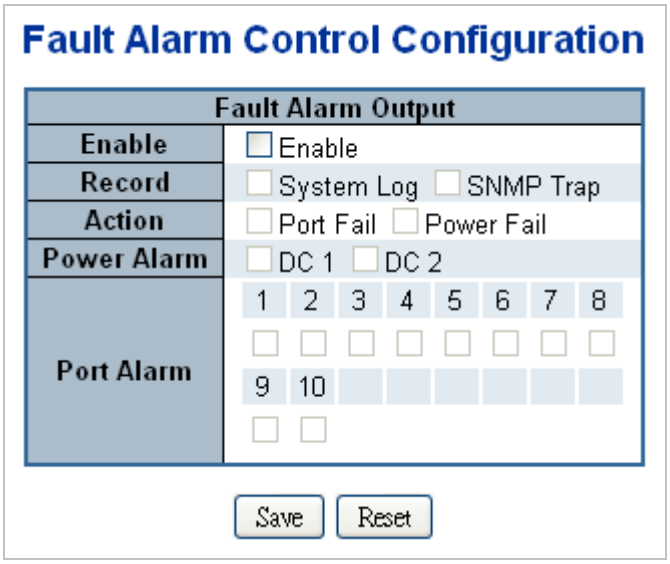


Figure 4-2-20 Windows File Selection Menu Popup

The page includes the following fields:

Object	Description
• **Enable**	Allows user to enable Fault Alarm function.
• **Record**	Allows user to record alarm message to System log, syslog or issues out via SNMP Trap or SMTP. As default SNMP Trap and SMTP are disabled, please enable them first if you want to issue alarm message via them.
• **Action**	Allows user to monitor and alarm from port failure or power failure.
• **Power Alarm**	Allows user to choose which power module that needs to be monitored.
• **Port Alarm**	Allows user to choose which port that needs to be monitored.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.18 EEE Power Reduction

This page allows the user to configure the current EEE port settings.

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization.

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted, all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP protocol.

For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until 3000 bytes of data is ready to be transmitted. For not introducing a large delay in case that data less than 3000 bytes shall be transmitted, data are always transmitted after 48 us, giving a maximum latency of 48 us + the wakeup time.

If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100Mbps full duplex mode.

The EEE Power Reduction screen in Figure 4-2-21 appears.

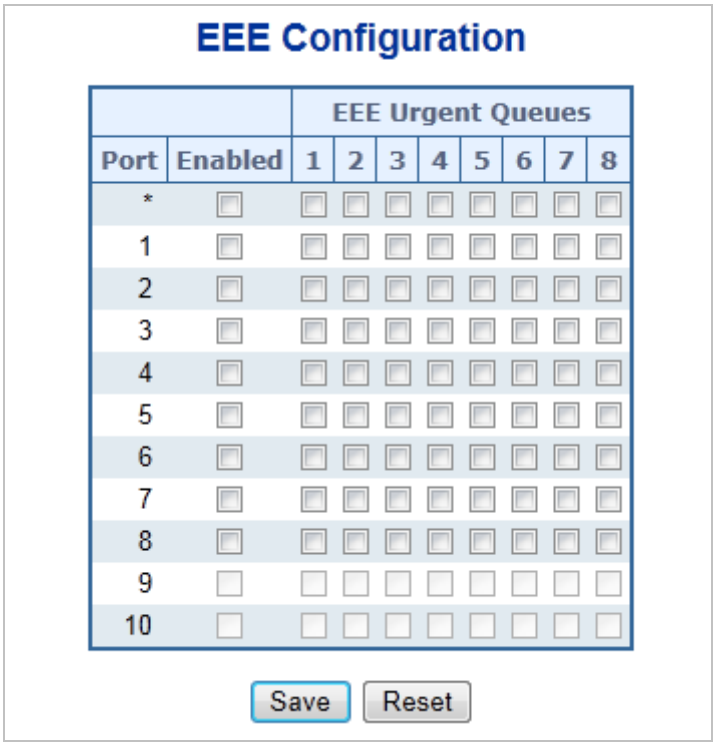


Figure 4-2-21: EEE Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical EEE port, * means to select all ports of Industrial Managed Switch.
• **EEE Enable**	Controls whether or not EEE is enabled for this switch port.
• **EEE Urgent Queues**	Queues set will activate transmission of frames as soon as any data is available. Otherwise, the queue will postpone the transmission until 3000 bytes, which are ready to be transmitted.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.2.19 Web Firmware Upgrade

This page facilitates an update on the firmware controlling the **Industrial Managed Switch**. The Web Firmware Upgrade screen in Figure 4-2-22 appears.

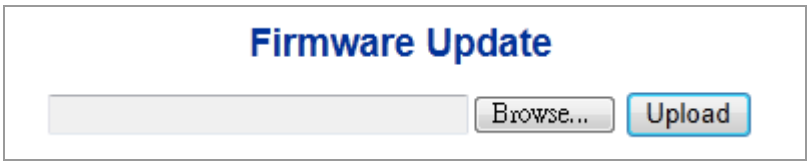


Figure 4-2-22: Web Firmware Upgrade Page Screenshot

To open **Firmware Upgrade** screen, perform the following:

1. Click **System** -> Web **Firmware Upgrade**.
2. The Firmware Upgrade screen is displayed as in Figure 4-2-22.
3. Click the "Browse "button of the main page, the system would pop up the file selection menu to choose firmware.
4. Select on the firmware and then click "Upload"; the **Software Upload Progress** would show the file upload status.
5. Once the software is loaded to the system successfully, the following screen appears. The system will load the new software after reboot.

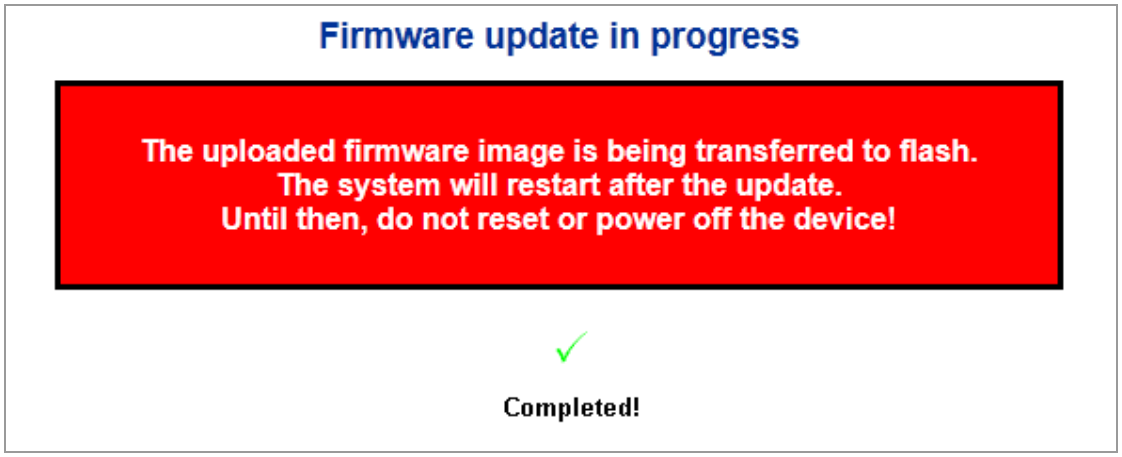

Firmware update in progress
The uploaded firmware image is being transferred to flash.
The system will restart after the update.
Until then, do not reset or power off the device!
Completed!

Figure 4-2-23: Software Successfully Loaded Notice Screen

Note

DO NOT Power OFF the **Industrial Managed Switch** until the update progress is complete.

Note

Do not quit the Firmware Upgrade page without pressing the "**OK**" button after the image is loaded. Or the system won't apply for the new firmware. User has to repeat the firmware upgrade processes again.

4.2.20 TFTP Firmware Upgrade

The **Firmware Upgrade** page provides the functions to allow a user to update the **Industrial Managed Switch** firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The TFTP Firmware Upgrade screen in Figure 4-2-24 appears.

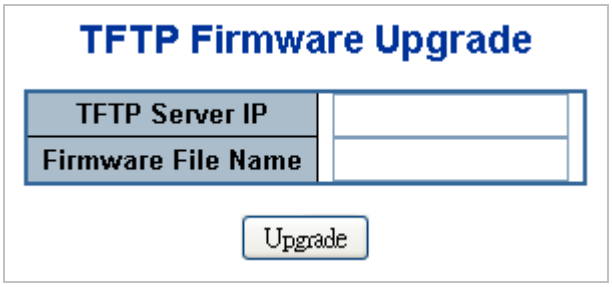


Figure 4-2-24: TFTP Firmware Update Page Screenshot

The page includes the following fields:

Object	Description
• **TFTP Server IP**	Fill in your TFTP server IP address.
• **Firmware File Name**	The name of firmware image. (Maximum length : 24 characters)

Buttons

Upgrade: Click to upgrade firmware.

DO NOT Power OFF the **Industrial Managed Switch** until the update progress is complete. Do not quit the Firmware Upgrade page without pressing the "**OK**" button after the image is loaded. Or the system won't apply for the new firmware. User has to repeat the firmware upgrade processes again.

4.2.21 Configuration Backup

This function allows backup and reload the current configuration of the **Industrial Managed Switch** to the local management station. The Configuration Backup screen in Figure 4-2-25 appears.

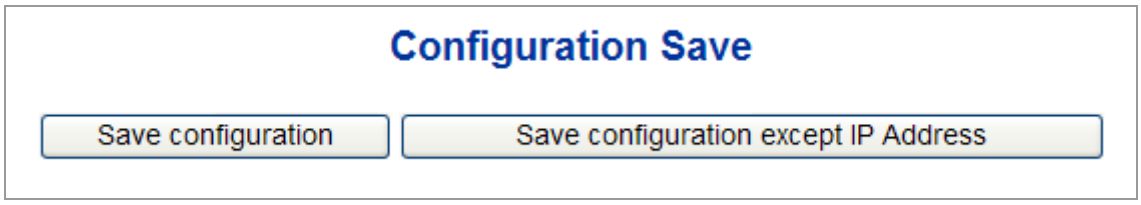


Figure 4-2-25: Configuration Save Page Screenshot

Save configuration except IP Address feature is almost the same as **Save configuration**, except the IP address, which will not be saved.

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:

Header tags:	<?xml version="1.0"?> and <configuration>. These tags are mandatory and must be present at the beginning of the file.
Section tags:	<platform>, <global> and <switch>. The platform section must be the first section tag and this section must include the correct platform ID and version. The global section is optional and includes configuration which is not related to specific switch ports. The switch section is optional and includes configuration which is related to specific switch ports.
Module tags:	<ip>, <mac>, <port> etc. These tags identify a module controlling specific parts of the configuration.
Group tags:	<port_table>, <vlan_table> etc. These tags identify a group of parameters, typically a table.
Parameter tags:	<mode>, <entry> etc. These tags identify parameters for the specific section, module and group. The <entry> tag is used for table entries.

Configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may then be modified using an editor and loaded to an **Industrial Managed Switch**.

The examples below show a small configuration file only including configuration of the MAC address age time and the learning mode per port. When loading this file, only the included parameters will be changed. This means that the age time will be set to 200 and the learn mode will be set to automatic.

■ **Save Configuration**

1. Press the **"Save Configuration"** button to save the current configuration in manager workstation. The following screens in Figure 4-2-26 & 4-2-27 appear

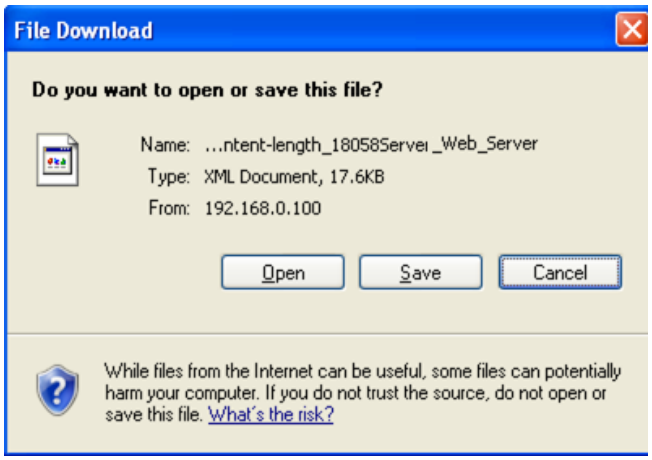

File Download
Do you want to open or save this file?
Name: ...ntent-length_18058Server_Web_Server
Type: XML Document, 17.6KB
From: 192.168.0.100
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 4-2-26: File Download Screen

2. Choose the file save path in management workstation.

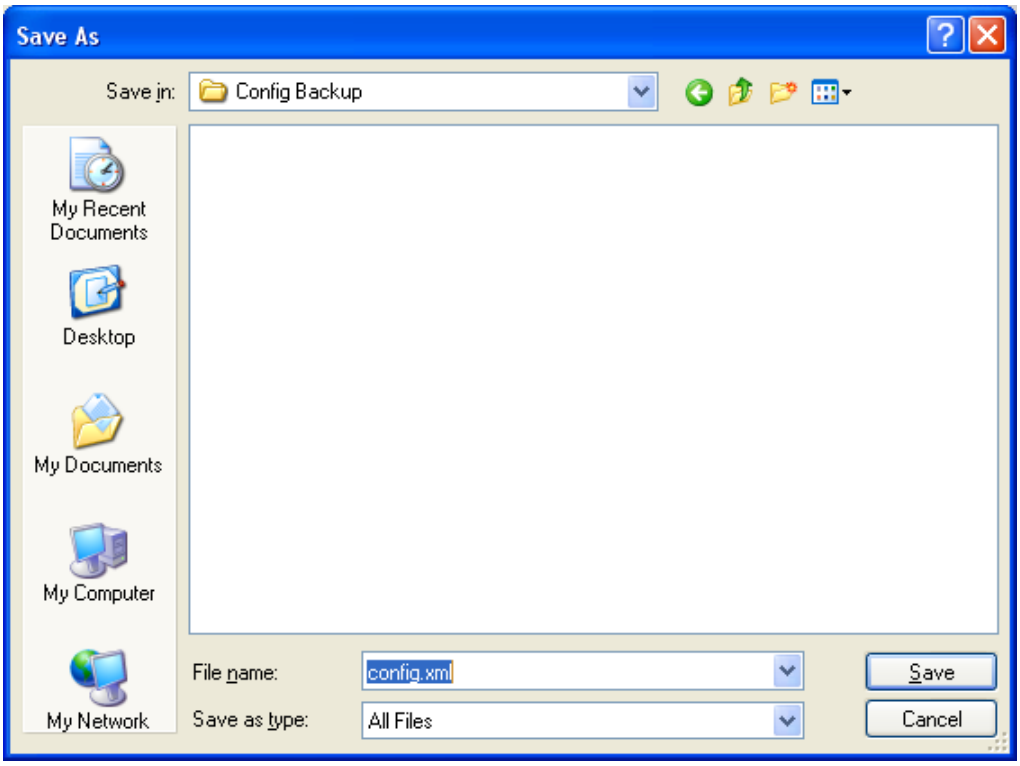


Figure 4-2-27: File Save Screen

4.2.22 Configuration Upload

This function allows backup and reload the current configuration of the **Industrial Managed Switch** to the local management station. The Configuration Upload screen in Figure 4-2-28 appears.

Figure 4-2-28: Configuration Upload Page Screenshot

- **Configuration Upload**

1. Click the "Browse" button of the main page, the system would pop up the file selection menu to choose saved configuration.

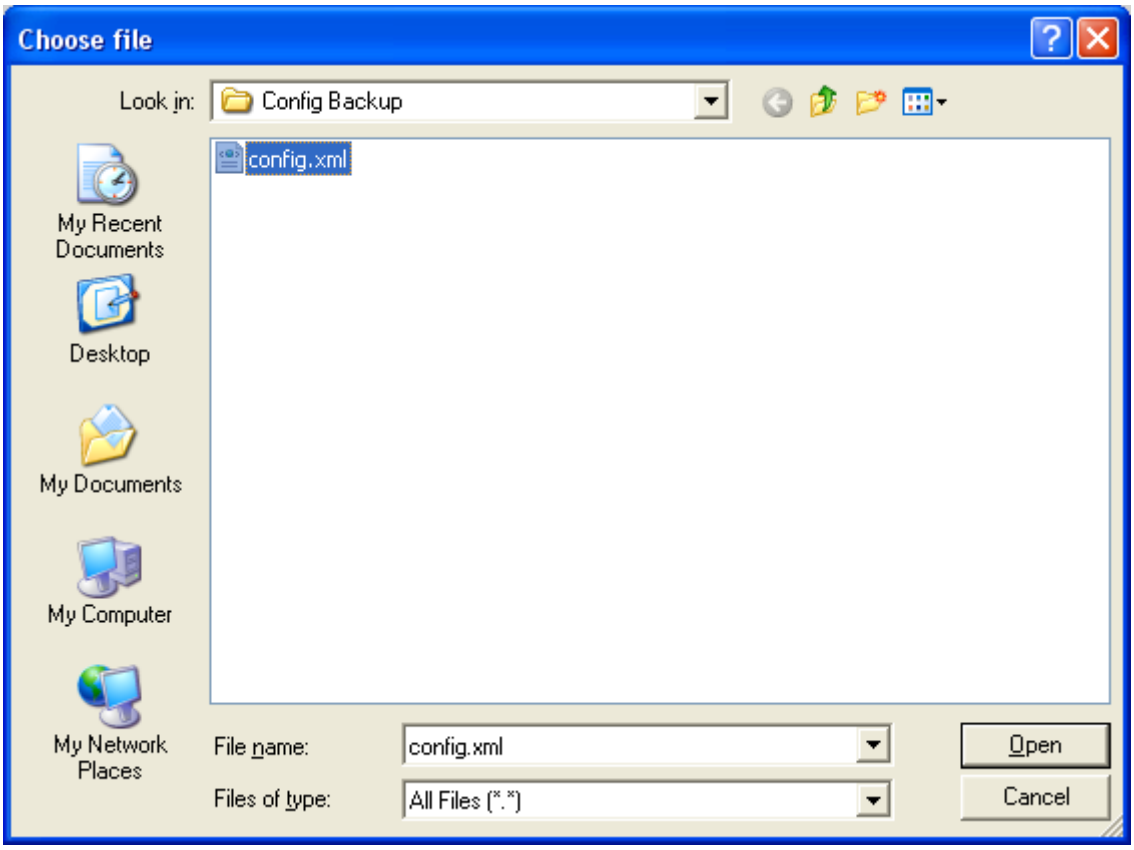


Figure 4-2-29: Windows File Selection Menu Popup

2. Select on the configuration file and then click "Upload", the bottom of the browser shows the upload status.

3. After down, the main screen appears "**Transfer Completed**".

4.2.23 Image Select

This function provides dual image deposit in the **Industrial Managed Switch**, user can select any one of the images as Active image of **Industrial Managed Switch.** The Image Select screen in Figure 4-2-30 appears.

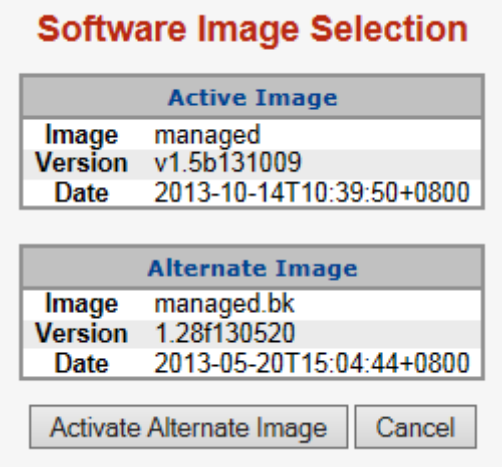


Figure 4-2-30: Image Select Page Screenshot

Button

Activate Alternate Image: Click to choose Alternate Image as Activate Image.

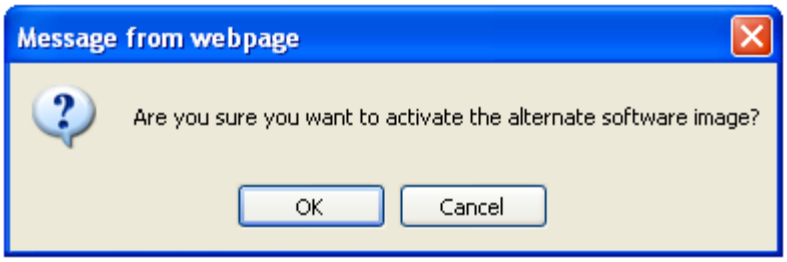


Figure 4-2-31: Image Select Page Screenshot

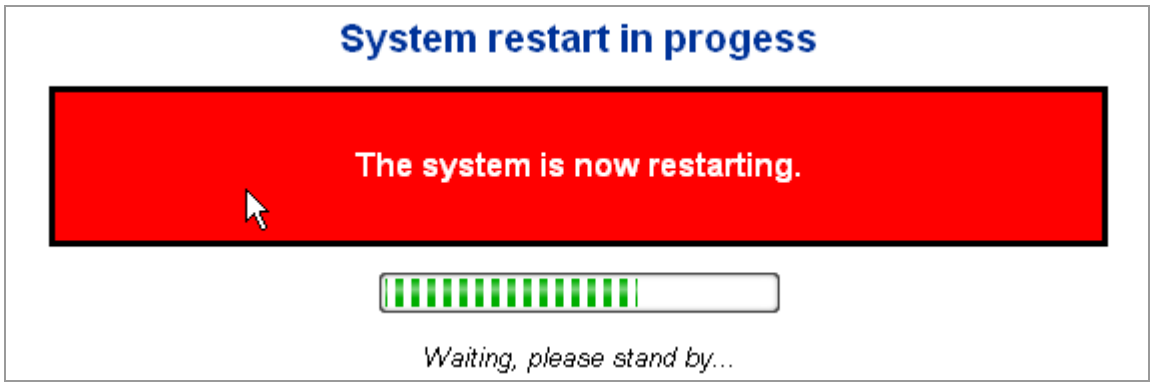


Figure 4-2-32: Image Select Page Screenshot

Figure 4-2-33: Image Select Page Screenshot

After the system reboot, you can use the Alternate Image of **Industrial Managed Switch**.

4.2.24 Factory Default

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in Figure 4-2-34 appears.

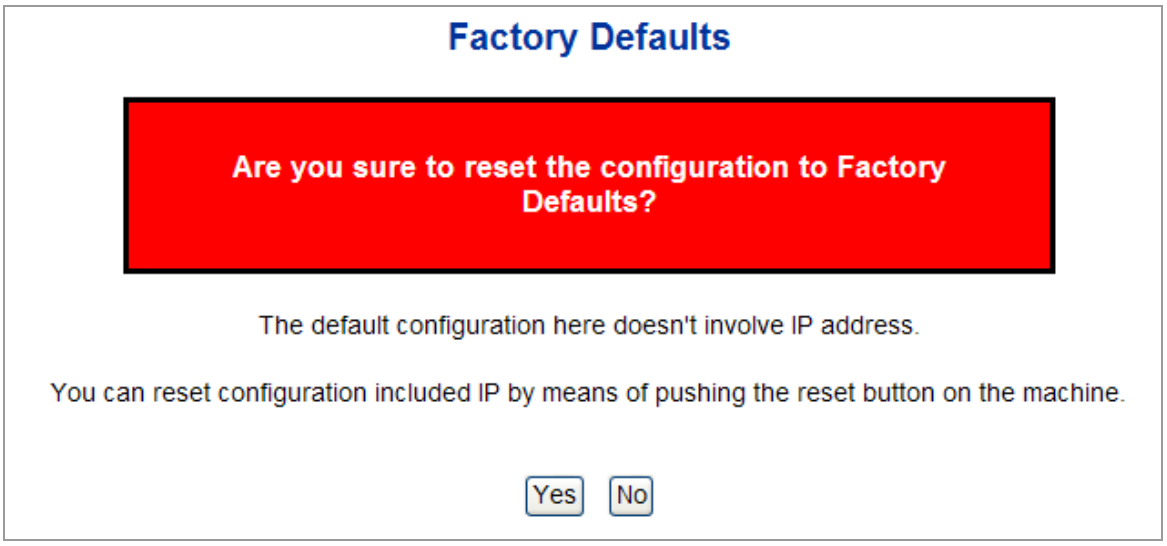

Factory Defaults
Are you sure to reset the configuration to Factory Defaults?
The default configuration here doesn't involve IP address.
You can reset configuration included IP by means of pushing the reset button on the machine.
Yes
No

Figure 4-2-34: Factory Default Page Screenshot

Buttons

Yes: Click to reset the configuration to Factory Defaults.

Figure 4-2-35: Factory Default Page Screenshot

No: Click to return to the web main page without resetting the configuration.

- After the "**Factory**" button is pressed and rebooted, the system will be loaded default settings, except IP address.

Note

To reset the Industrial Managed Switch to the Factory default setting, you can also press the hardware reset button at the front panel for about more than 10 seconds. After the device is rebooted, all configurations will be loaded to default setting including IP address. You can login the management WEB interface within the same subnet of 192.168.0.xx.

4.2.25 System Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user will re-access the WEB interface about 60 seconds later. The System Reboot screen in Figure 4-2-36 appears.

Figure 4-2-36: System Reboot Page Screenshot

Buttons

Yes: Click to reboot the system.

No: Click to return to the web main page without rebooting the system.

4.3 Simple Network Management Protocol

4.3.1 SNMP Overview

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management information base (MIB) and network-management protocol：

- **Network management stations (NMSs)** ：Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents**：Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)** ：A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **Network-management protocol**：A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get --** Allows the NMS to retrieve an object instance from the agent.
- **Set --** Allows the NMS to set values for object instances within an agent.
- **Trap --** Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- **Write** = private
- **Read** = public

Use the SNMP Menu to display or configure the Managed Switch's SNMP function. This section has the following items:

- **System Configuration** Configure SNMP on this page.
- **System Information** The system information is provides here.
- **SNMPv3 Communities** Configure SNMPv3 communities table on this page.
- **SNMPv3 Users** Configure SNMPv3 users table on this page.
- **SNMPv3 Groups** Configure SNMPv3 groups table on this page.

- **SNMPv3 Views** Configure SNMPv3 views table on this page.
- **SNMPv3 Accesses** Configure SNMPv3 accesses table on this page.

4.3.2 SNMP System Configuration

Configure SNMP on this page. The SNMP System Configuration screen in Figure 4-3-1 appears.

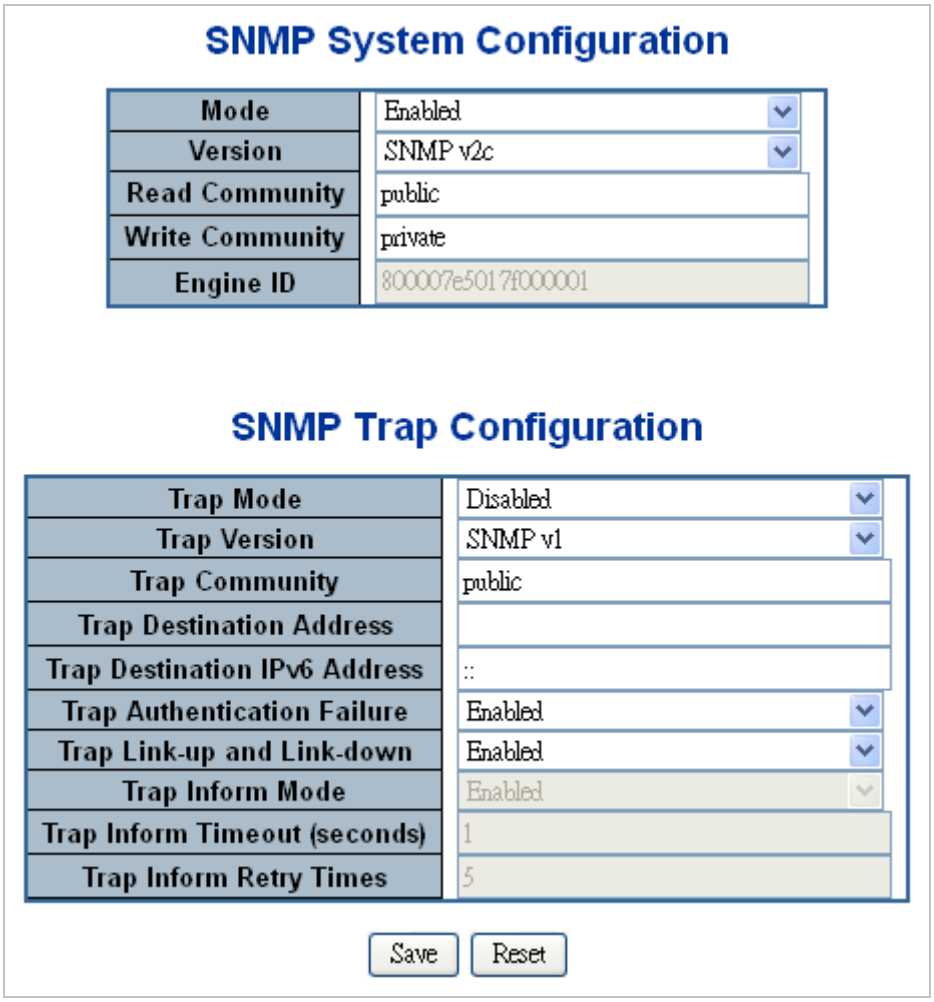


Figure 4-3-1: SNMP System Configuration Page Screenshot

The SNMP System Configuration page includes the following fields:

Object	Description
• **Mode**	Indicates the SNMP mode operation. Possible modes are: ■ **Enabled**: Enable SNMP mode operation. ■ **Disabled**: Disable SNMP mode operation.
• **Version**	Indicates the SNMP supported version. Possible versions are: ■ **SNMP v1**: Set SNMP supported version 1. ■ **SNMP v2c**: Set SNMP supported version 2c. ■ **SNMP v3**: Set SNMP supported version 3.
• **Read Community**	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a

	particular range of source addresses can be used to restrict source subnet.
• **Write Community**	Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
• **Engine ID**	Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

The SNMP Trap Configuration page includes the following fields:

Object	Description
• **Trap Mode**	Indicates the SNMP trap mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap mode operation. ■ **Disabled**: Disable SNMP trap mode operation.
• **Trap Version**	Indicates the SNMP trap supported version. Possible versions are: ■ **SNMP v1**: Set SNMP trap supported version 1. ■ **SNMP v2c**: Set SNMP trap supported version 2c. ■ **SNMP v3**: Set SNMP trap supported version 3.
• **Trap Community**	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
• **Trap Destination Address**	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.
• **Trap Destination IPv6 Address**	Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '192.1.2.34'.
• **Trap Authentication Failure**	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: ■ **Enabled**: Enable SNMP trap authentication failure. ■ **Disabled**: Disable SNMP trap authentication failure.
• **Trap Link-up and Link-down**	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap link-up and link-down mode operation. ■ **Disabled**: Disable SNMP trap link-up and link-down mode operation.
• **Trap Inform Mode**	Indicates the SNMP trap inform mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap inform mode operation. ■ **Disabled**: Disable SNMP trap inform mode operation.
• **Trap Inform Timeout (seconds)**	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
• **Trap Inform Retry Times**	Indicates the SNMP trap informs retry times. The allowed range is 0 to 255.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.3 SNMP System Information

The switch system information is provided here. The SNMP System Information screen in Figure 4-3-2 appears.

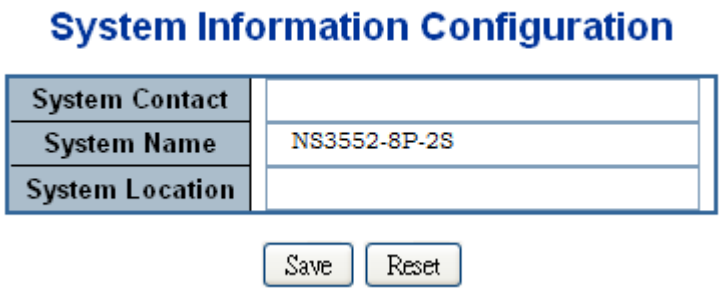


Figure 4-3-2: System Information Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **System Contact**	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
• **System Name**	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
• **System Location**	The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.4 SNMPv3 Configuration

4.3.4.1 SNMPv3 Communities

Configure SNMPv3 communities table on this page. The entry index key is Community. The SNMPv3 Communities screen in Figure 4-3-3 appears.

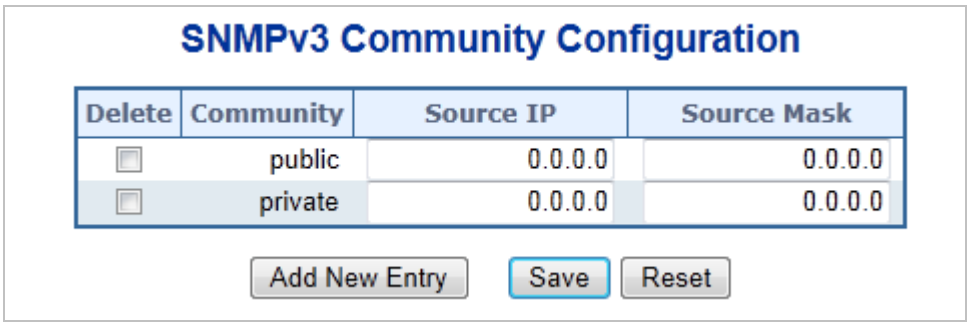


Figure 4-3-3: SNMPv3 Communities Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Community**	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
• **Source IP**	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
• **Source Mask**	Indicates the SNMP access source address mask.

Buttons

Add New User: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.4.2 SNMPv3 Users

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name. The SNMPv3 Users screen in Figure 4-3-4 appears.

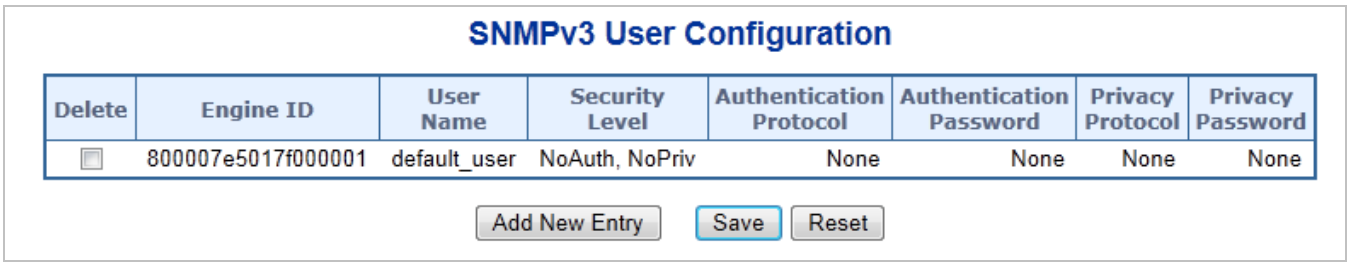


Figure 4-3-4: SNMPv3 Users Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Engine ID**	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: ■ **NoAuth, NoPriv**: None authentication and none privacy. ■ **Auth, NoPriv**: Authentication and none privacy. ■ **Auth, Priv**: Authentication and privacy. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
• **Authentication Protocol**	Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are: ■ **None**: None authentication protocol. ■ **MD5**: An optional flag to indicate that this user using MD5 authentication protocol. ■ **SHA**: An optional flag to indicate that this user using SHA authentication protocol. ■ The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
• **Authentication Password**	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
• **Privacy Protocol**	Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are: ■ **None**: None privacy protocol. ■ **DES**: An optional flag to indicate that this user using DES authentication protocol.
• **Privacy Password**	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

Add New User: Click to add a new user entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.4.3 SNMPv3 Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name. The SNMPv3 Groups screen in Figure 4-3-5 appears.

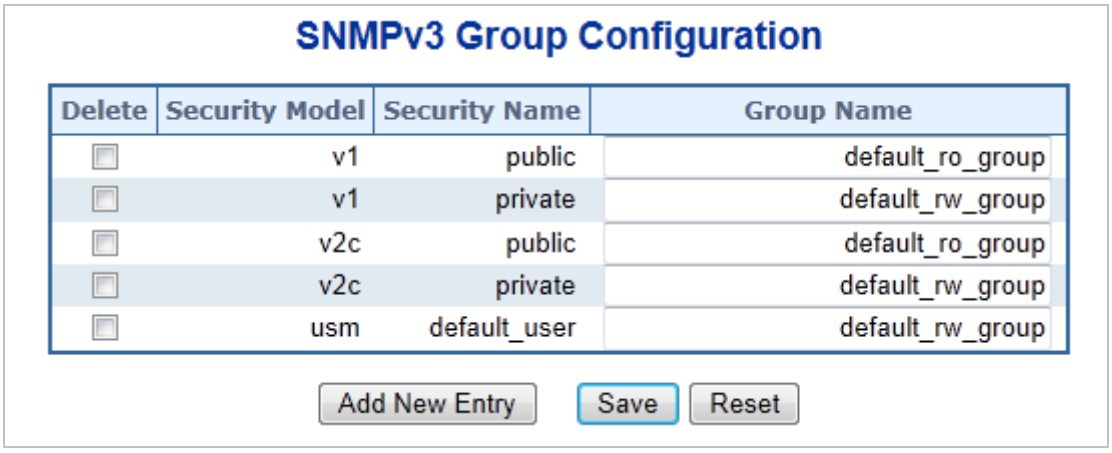


Figure 4-3-5: SNMPv3 Groups Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are: ■ **v1**: Reserved for SNMPv1. ■ **v2c**: Reserved for SNMPv2c. ■ **usm**: User-based Security Model (USM).
• **Security Name**	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

Add New User: Click to add a new group entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.4.4 SNMPv3 Views

Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Subtree. The SNMPv3 Views screen in Figure 4-3-6 appears.

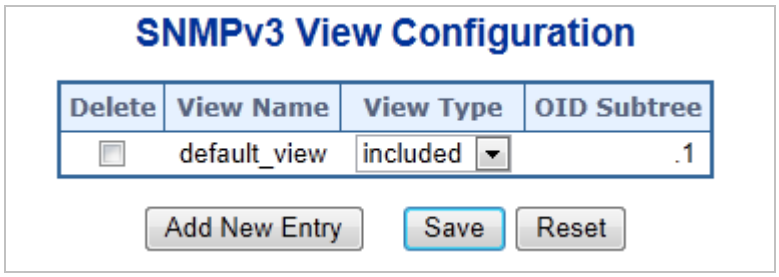


Figure 4-3-6: SNMPv3 Views Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **View Name**	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **View Type**	Indicates the view type that this entry should belong to. Possible view type are: ■ **included**: An optional flag to indicate that this view subtree should be included. ■ **excluded**: An optional flag to indicate that this view subtree should be excluded. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.
• **OID Subtree**	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

Add New User: Click to add a new view entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.3.4.5 SNMPv3 Access

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.

The SNMPv3 Access screen in Figure 4-3-7 appears.

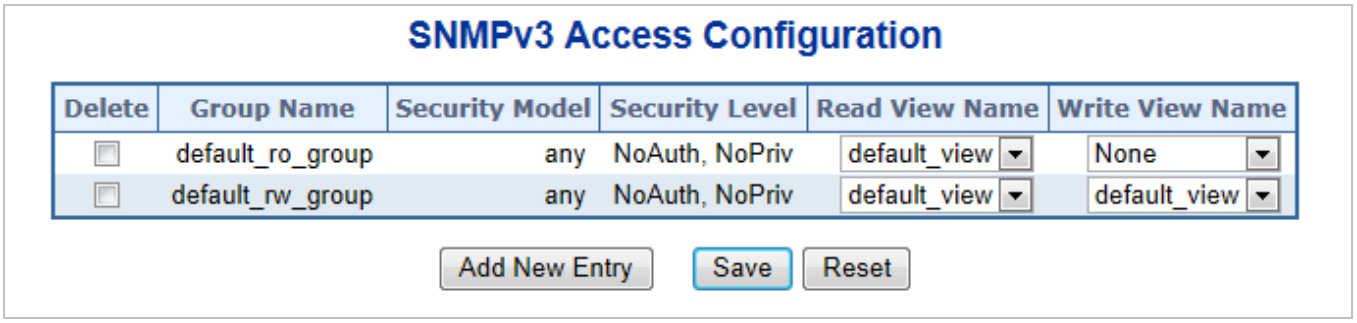


Figure 4-3-7: SNMPv3 Accesses Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Group Name**	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Security Model**	Indicates the security model that this entry should belong to. Possible security models are: ■ **any**: Accepted any security model (v1|v2c|usm). ■ **v1**: Reserved for SNMPv1. ■ **v2c**: Reserved for SNMPv2c. ■ **usm**: User-based Security Model (USM)
• **Security Level**	Indicates the security model that this entry should belong to. Possible security models are: ■ **NoAuth, NoPriv**: None authentication and none privacy. ■ **Auth, NoPriv**: Authentication and none privacy. ■ **Auth, Priv**: Authentication and privacy.
• **Read View Name**	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Write View Name**	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

Add New User: Click to add a new access entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.4 Port Management

Use the Port Menu to display or configure the Managed Switch's ports. This section has the following items:

- **Port Configuration** Configures port connection settings
- **Port Statistics Overview** Lists Ethernet and RMON port statistics
- **Port Statistics Detail** Lists Ethernet and RMON port statistics
- **SFP Information** Display SFP information
- **Port Mirror** Sets the source and target ports for mirroring

4.4.1 Port Configuration

This page displays current port configurations. Ports can also be configured here. The Port Configuration screen in Figure 4-4-1 appears.

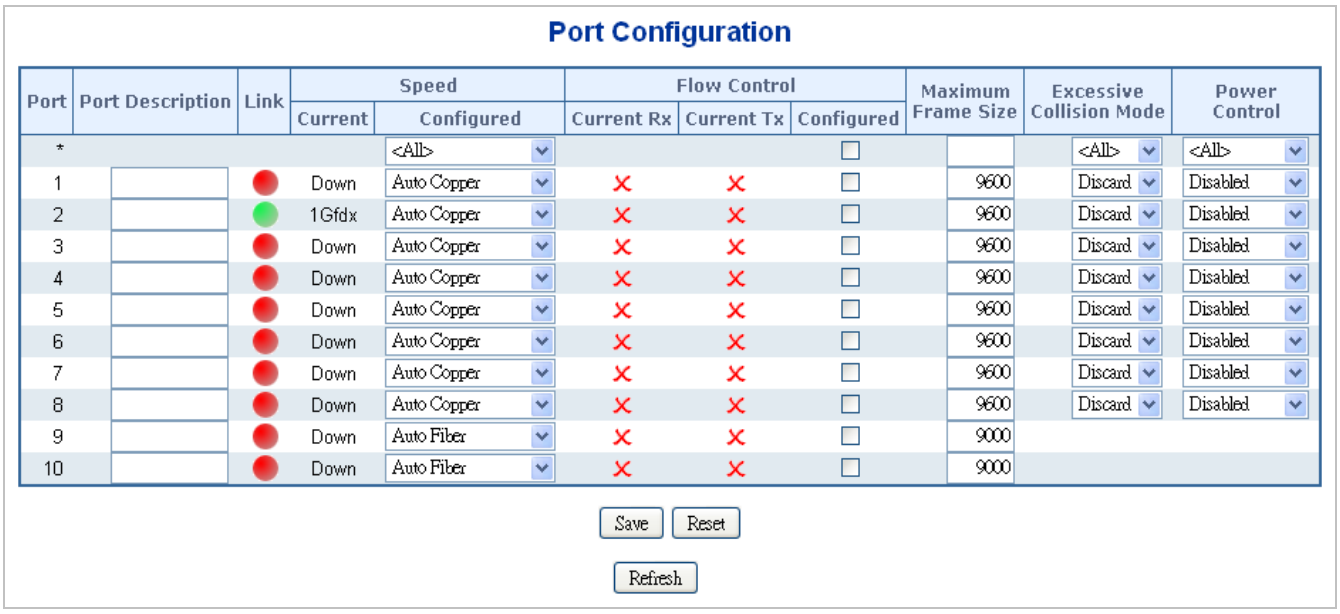


Figure 4-4-1: Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row, * means selection all ports of Industrial Managed Switch.
• **Port Description**	This function provides input per port description and the available letters is 12.
• **Link**	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
• **Current Link Speed**	Provides the current link speed of the port.

• **Configured Link Speed**	Select any available link speed for the given switch port. Draw the menu bar to select the mode. ■ **All**- Setup whole ports with the same setting. ■ **Auto Copper** - Setup Auto negotiation. ■ **Auto Fiber** - Setup Auto negotiation. ■ **10 Half** - Force sets 10Mbps/Half-Duplex mode. ■ **10 Full** - Force sets 10Mbps/Full-Duplex mode. ■ **100 Half** - Force sets 100Mbps/Half-Duplex mode. ■ **100 Full** - Force sets 100Mbps/Full-Duplex mode. ■ **1000 Full** - Force sets 10000Mbps/Full-Duplex mode. ■ **Disable** - Shutdown the port manually.
• **Flow Control**	When **Auto Speed** is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
• **Maximum Frame Size**	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes for TP port and 9000 bytes for Fiber port.
• **Excessive Collision Mode**	Configure port transmit collision behavior. ■ **Discard**: Discard frame after 16 collisions (default). ■ **Restart**: Restart back off algorithm after 16 collisions.
• **Power Control**	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. ■ **Disabled**: All power savings mechanisms disabled. ■ **ActiPHY**: Link down power savings enabled. ■ **PerfectReach**: Link up power savings enabled. ■ **Enabled**: Both link up and link down power savings enabled.

When setting each port to run at 100M Full, 100M Half, 10M Full, and 10M Half-speed modes, the Auto-MDIX function will disable.

Buttons

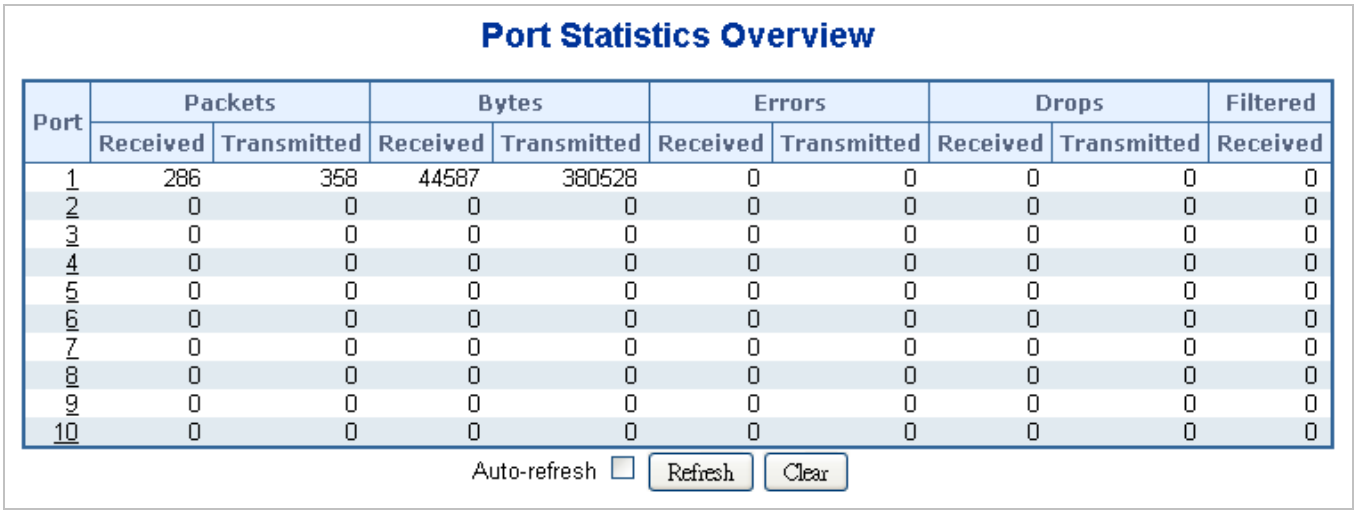
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page. Any changes made locally will be undone.

4.4.2 Port Statistics Overview

This page provides an overview of general traffic statistics for all switch ports. The Port Statistics Overview screen in Figure 4-4-2 appears.



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	286	358	44587	380528	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

Auto-refresh Refresh Clear

Figure 4-4-2: Port Statistics Overview Page Screenshot

The displayed counters are:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Packets**	The number of received and transmitted packets per port.
• **Bytes**	The number of received and transmitted bytes per port.
• **Errors**	The number of frames received in error and the number of incomplete transmissions per port.
• **Drops**	The number of frames discarded due to ingress or egress congestion.
• **Filtered**	The number of received frames filtered by the forwarding process.

Buttons

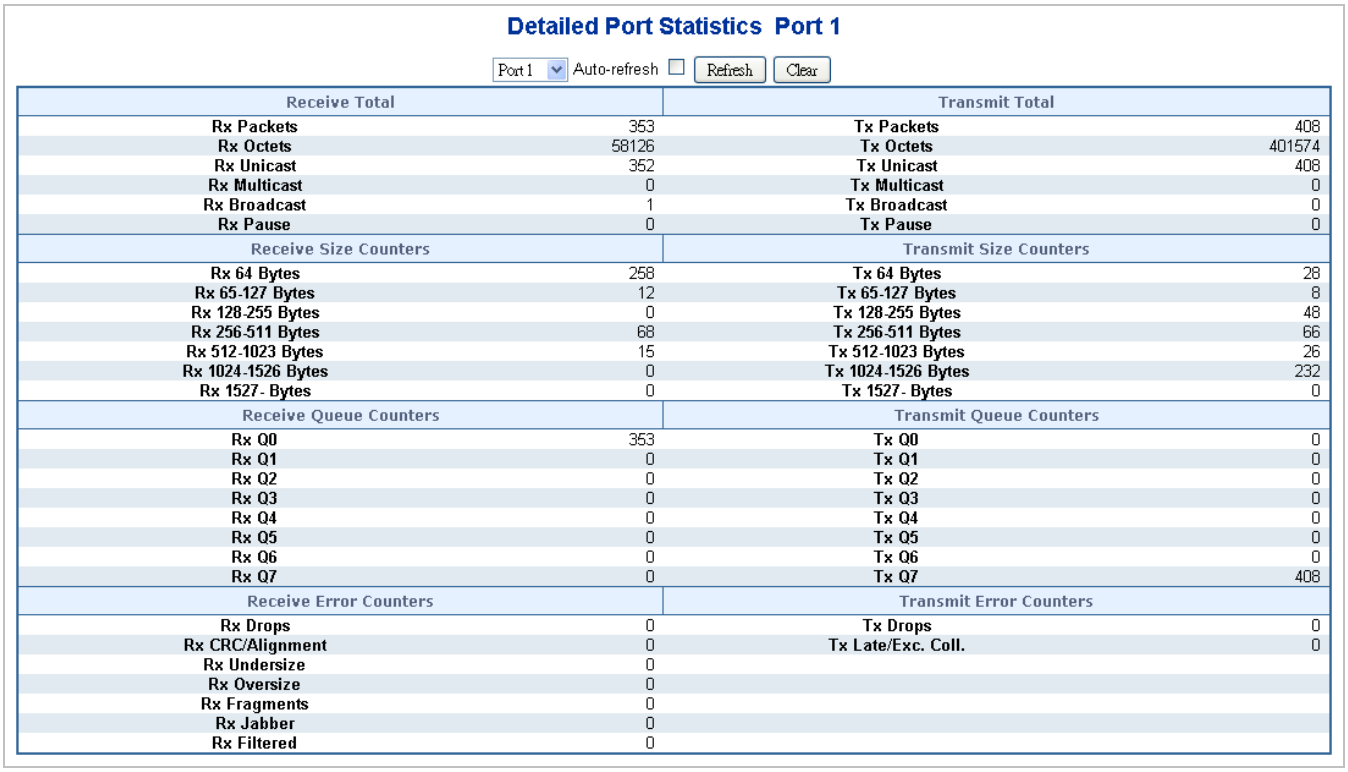
Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

4.4.3 Port Statistics Detail

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The selected port is belonging to the currently selected stack unit, as reflected by the page header. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. The Port Statistics Detail screen in Figure 4-4-3 appears.



Receive Total		Transmit Total	
Rx Packets	353	Tx Packets	408
Rx Octets	58126	Tx Octets	401574
Rx Unicast	352	Tx Unicast	408
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	1	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	258	Tx 64 Bytes	28
Rx 65-127 Bytes	12	Tx 65-127 Bytes	8
Rx 128-255 Bytes	0	Tx 128-255 Bytes	48
Rx 256-511 Bytes	68	Tx 256-511 Bytes	66
Rx 512-1023 Bytes	15	Tx 512-1023 Bytes	26
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	232
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	353	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	408
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Figure 4-4-3: Detailed Port Statistics Port 1 Page Screenshot

The page includes the following fields:

Receive Total and Transmit Total

Object	Description
• **Rx and Tx Packets**	The number of received and transmitted (good and bad) packets
• **Rx and Tx Octets**	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
• **Rx and Tx Unicast**	The number of received and transmitted (good and bad) unicast packets.
• **Rx and Tx Multicast**	The number of received and transmitted (good and bad) multicast packets.
• **Rx and Tx Broadcast**	The number of received and transmitted (good and bad) broadcast packets.
• **Rx and Tx Pause**	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The numeric of received and transmitted packet is per input and output queue.

Receive Error Counters

Object	Description
• **Rx Drops**	The numeric of frames is dropped due to lack of receive buffers or egress congestion.
• **Rx CRC/Alignment**	The number of frames received with CRC or alignment errors.
• **Rx Undersize**	The number of short[1] frame received with valid CRC.
• **Rx Oversize**	The number of long[2] frame received with valid CRC.
• **Rx Fragments**	The number of short[1] frame received with invalid CRC.
• **Rx Jabber**	The number of long[2] frame received with invalid CRC.
• **Rx Filtered**	The number of received frames filtered by the forwarding process. Short frames are frames that are smaller than 64 bytes. Long frames are frames that are longer than the configured maximum frame length for this port.

1 Short frame is the frames that are smaller than 64 bytes.
2 Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Object	Description
• **Tx Drops**	The number of frames dropped due to output buffer congestion.
• **Tx Late/Exc. Coll.**	The number of frames dropped due to excessive or late collisions.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

4.4.4 SFP Information

You can check the physical or operational status of an SFP module via the SFP Module Information page. This page shows the operational status, such as the transceiver type, speed, and wavelength and supports distance of SFP module on a specific interface. You can also use the hyperlink of port no. to check the statistics on a specific interface. The SFP Module Information

screen in Figure 4-4-4 appears.

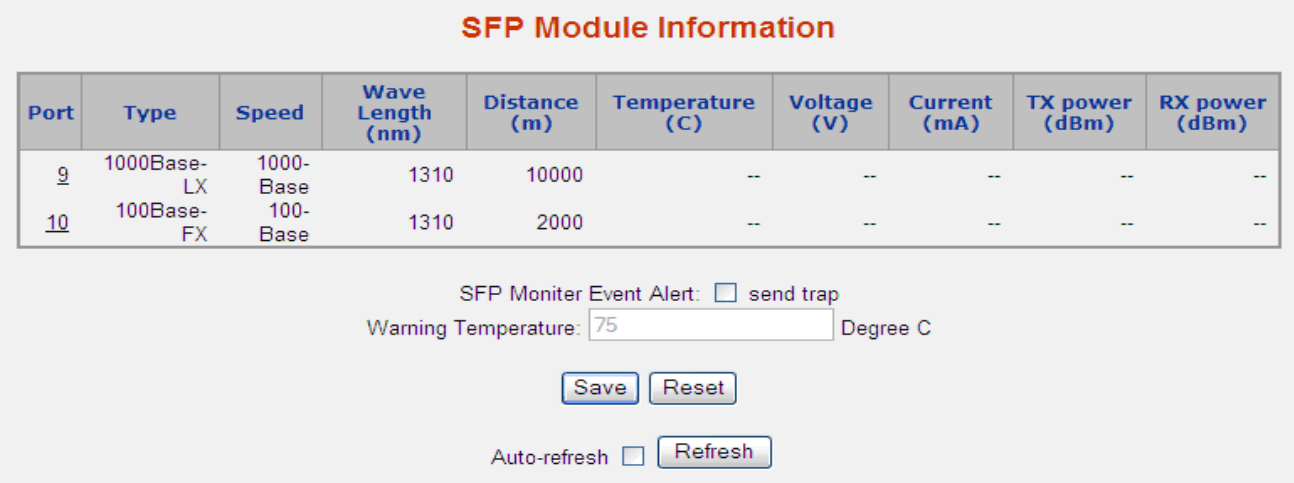


Figure 4-4-4: SFP Module Information for Switch Page Screenshot

The page includes the following fields:

Object	Description
• **Type**	Display the type of current SFP module; the possible types are: ■ 1000Base-SX ■ 1000Base-LX ■ 100Base-FX
• **Speed**	Display the speed of current SFP module. The speed value or description is gotten from the SFP module. Different vendors of SFP modules might show different speed information.
• **Wave Length(nm)**	Display the wavelength of current SFP module. The wavelength value is gotten from the SFP module. Use this column to check if the wavelength values of two nodes are matched while the fiber connection is failed.
• **Distance(m)**	Display the support distance of current SFP module. The distance value is gotten from the SFP module.
• **Temperature (C)**	Display the temperature of current SFP module. The temperature value is gotten from the SFP module.
• **Voltage (V)**	Display the voltage of current SFP module. The voltage value is gotten from the SFP module.
• **Current (mA)**	Display the ampere of current SFP module. The ampere value is gotten from the SFP module.
• **TX Power (dBm)**	Display the TX power of current SFP module. The TX power value is gotten from the SFP module.
• **RX Power (dBm)**	Display the RX power of the current SFP module. The RX power value is gotten from the SFP module.

Buttons

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

4.4.5 Port Mirror

Configure port Mirroring on this page. This function provide to monitoring network traffic that forwards a copy of each incoming or outgoing packet from one port of a network Switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

- To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.
- The Managed Switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

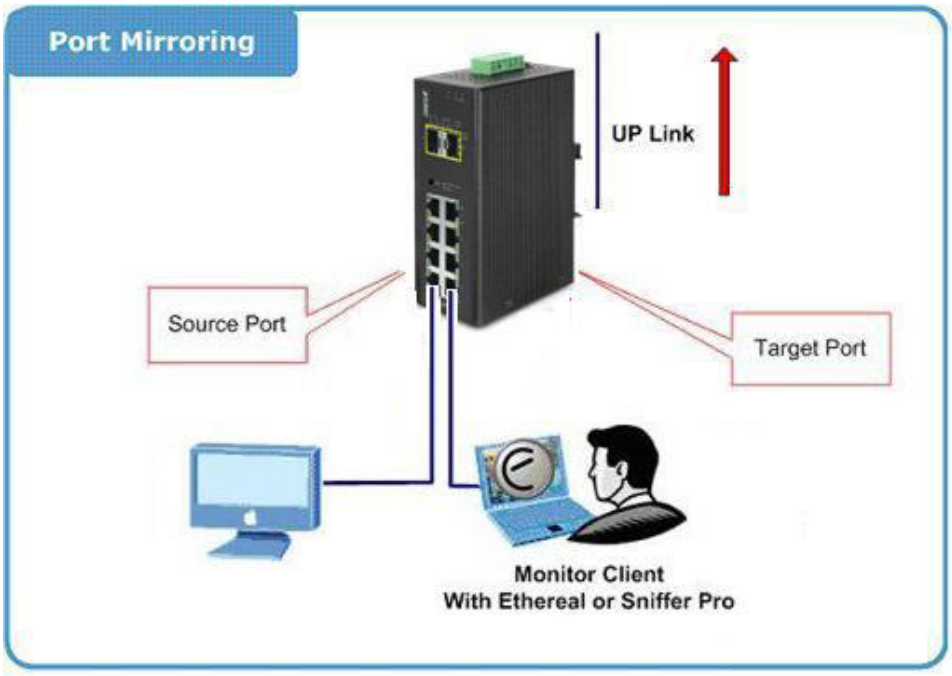


Figure 4-4-5: Port Mirror Application

The traffic to be copied to the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

- **Mirror Port Configuration**

The Port Mirror screen in Figure 4-4-6 appears.

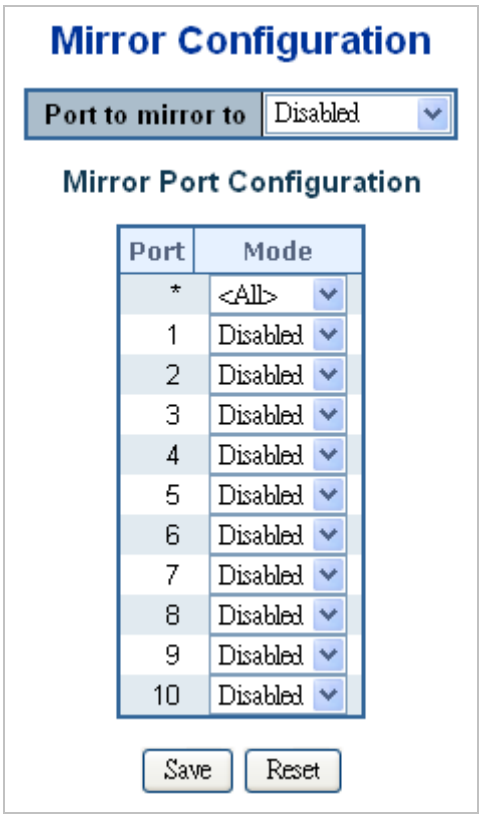


Figure 4-4-6: Mirror Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port to mirror on**	**Port to mirror** also known as the **mirror port**. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. **Disabled** disables mirroring.
• **Port**	The logical port for the settings contained in the same row, * means selection all ports of Industrial Managed Switch.
• **Mode**	Select mirror mode. ■ **Rx only**: Frames received at this port are mirrored to the mirroring port. Frames transmitted are not mirrored. ■ **Tx only**: Frames transmitted from this port are mirrored to the mirroring port. Frames received are not mirrored. ■ **Disabled**: Neither frames transmitted nor frames received are mirrored. ■ **Both**: Frames received and frames transmitted are mirrored to the mirror port.

For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the **mirror port**. Because of this, **mode** for the selected mirror port is limited to **Disabled** or **Rx only**.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5 Link Aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated Links can be assigned manually (**Port Trunk**) or automatically by enabling Link Aggregation Control Protocol (**LACP**) on the relevant links.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, Duplex setting, etc.

The device supports the following Aggregation links :

- **Static LAGs** (**Port Trunk**) – Force aggregared selected ports to be a trunk group.
- **Link Aggregation Control Protocol** (**LACP**) LAGs - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

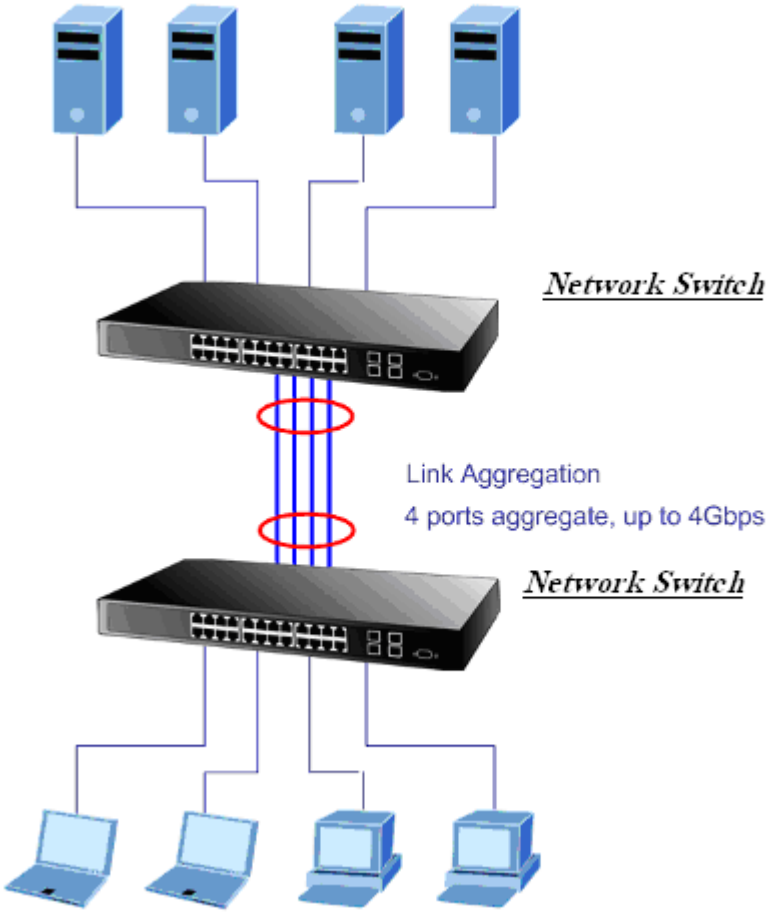


Figure 4-5-1: Link Aggregation Topology

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems that require high speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refer to the IEEE 802.3ad standard.

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ-45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to

avoid creating a data loop.

It allows a maximum of 10 ports to be aggregated at the same time. The Managed Switch support Gigabit Ethernet ports (up to 5 groups). If the group is defined as a LACP static link aggregationing group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregationing group, then the number of ports must be the same as the group member ports.

The aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Reording of frames within a flow is therefore not possible. The aggregation code is based on the following information:

- **Source MAC**
- **Destination MAC**
- **Source and destination IPv4 address.**
- **Source and destination TCP/UDP ports for IPv4 packets**

Normally, all 5 contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 10 member ports. Any quantity of link aggregation s may be configured for the device (only limited by the quantity of ports on the device.) To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

4.5.1 Static Aggregation

This page is used to configure the Aggregation hash mode and the aggregation group. The aggregation hash mode settings are global, whereas the aggregation group relate to the currently selected stack unit, as reflected by the page header.

Hash Code Contributors

The Static Aggregation screen in Figure 4-5-2 appears.

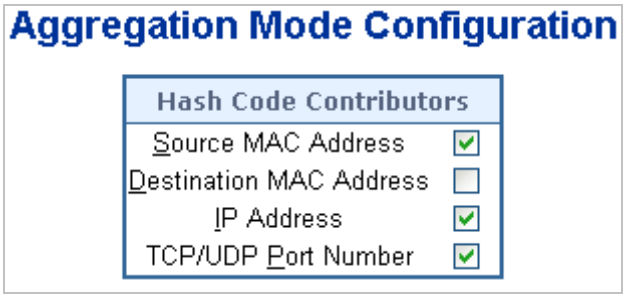


Figure 4-5-2 : Aggregation Mode Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Source MAC Address**	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is **enabled**.
• **Destination MAC Address**	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is **disabled**.
• **IP Address**	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is **enabled**.
• **TCP/UDP Port Number**	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is **enabled**.

Static Aggregation Group Configuration

The Aggregation Group Configuration screen in Figure 4-5-3 appears.

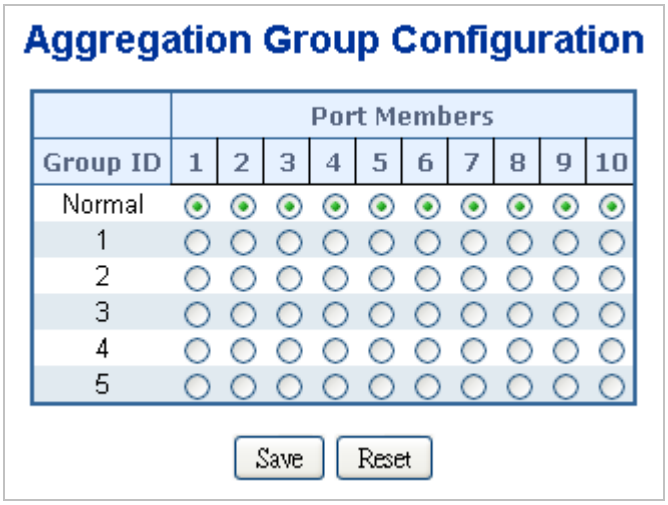


Figure 4-5-3: Aggregation Group Configuration Page Screenshot

The page includes the following fields:

.Object	Description
• **Group ID**	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
• **Port Members**	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.2 LACP Configuration

Link Aggregation Control Protocol (LACP) - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. LACP allows switches connected to each other to discover automatically whether any ports are member of the same LAG.

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. The LACP port settings relate to the currently selected stack unit, as reflected by the page header. The LACP Configuration screen in Figure 4-5-4 appears.

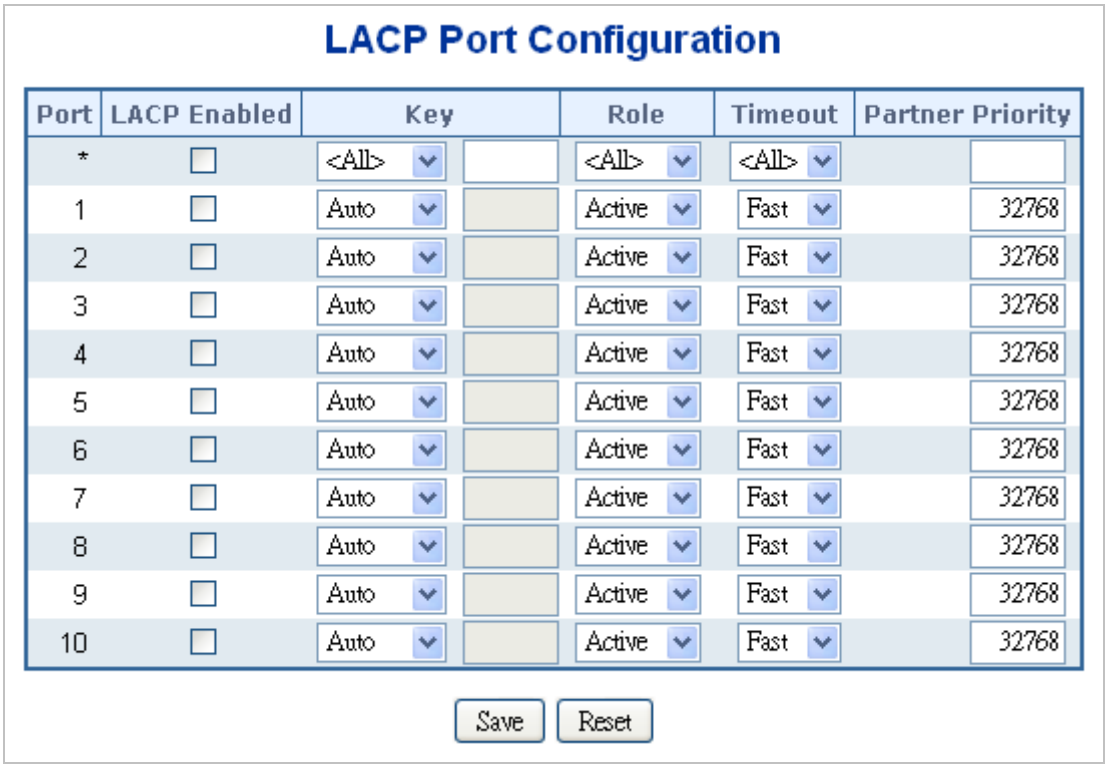


Figure 4-5-4 : LACP Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number, * means selection all ports of Industrial Managed Switch.
• **LACP Enabled**	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.
• **Key**	The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. The default setting is "**Auto**"
• **Role**	The Role shows the LACP activity status. The Active will transmit LACP packets each second; while Passive will wait for a LACP packet from a partner (speak if spoken to).
• **Timeout**	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

• **Partner Priority**	The `Prior` controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.5.3 LACP System Status

This page provides a status overview for all LACP instances. The LACP Status page displays the current LACP aggregation Groups and LACP Port status. The LACP System Status screen in Figure 4-5-5 appears.

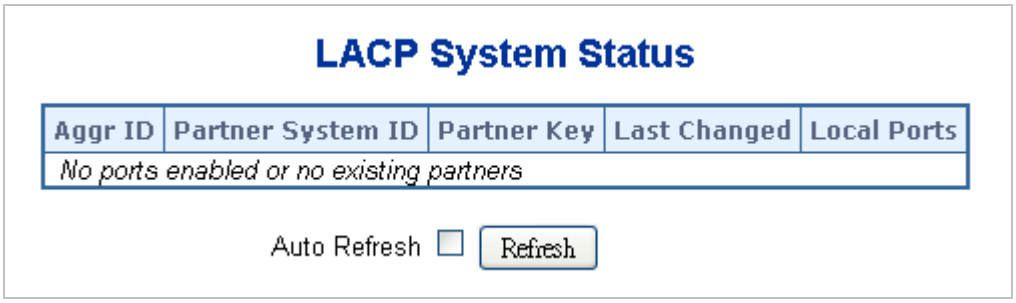


Figure 4-5-5: LACP System Status Page Screenshot

The page includes the following fields:

Object	Description
• **Aggr ID**	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
• **Partner System ID**	The system ID (MAC address) of the aggregation partner.
• **Partner Key**	The Key that the partner has assigned to this aggregation ID.
• **Last changed**	The time since this aggregation changed.
• **Local Ports**	Shows which ports are a part of this aggregation for this switch. .

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Automatic refresh occurs every 3 seconds.

4.5.4 LACP Port Status

This page provides a status overview for LACP status for all ports. The LACP Port Status screen in Figure 4-5-6 appears.

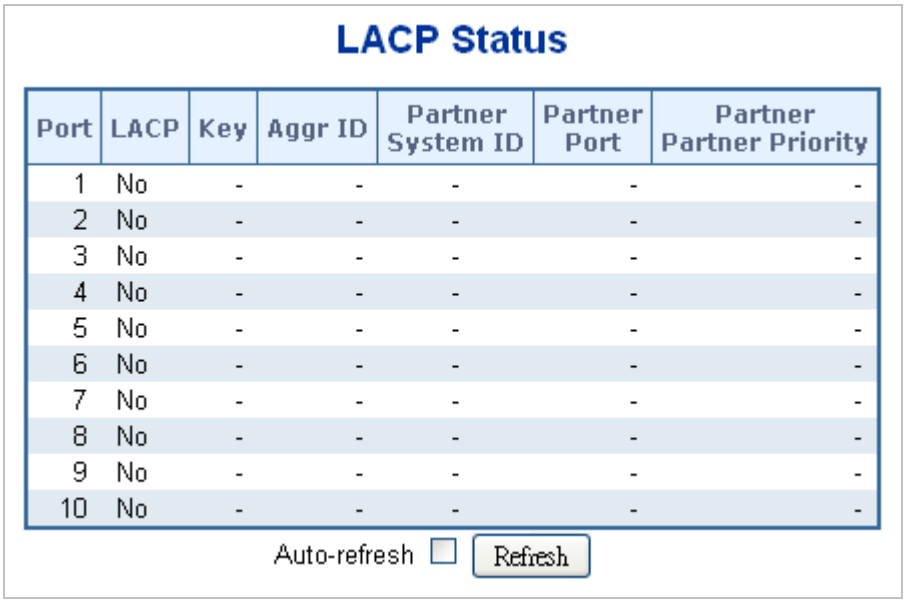

LACP Status
Port
LACP
Key
Aggr ID
Partner System ID
Partner Port
Partner Partner Priority
1 No - - - - -
2 No - - - - -
3 No - - - - -
4 No - - - - -
5 No - - - - -
6 No - - - - -
7 No - - - - -
8 No - - - - -
9 No - - - - -
10 No - - - - -
Auto-refresh
Refresh

Figure 4-5-6: LACP Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **LACP**	'**Yes**' means that LACP is enabled and the port link is up. '**No**' means that LACP is not enabled or that the port link is down. '**Backup**' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
• **Key**	The key assigned to this port. Only ports with the same key can aggregate together.
• **Aggr ID**	The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
• **Partner System ID**	The partners System ID (MAC address).
• **Partner Port**	The partner port number connected to this port.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Automatic refresh occurs every 3 seconds.

4.5.5 LACP Port Statistics

This page provides an overview for LACP statistics for all ports. The LACP Port Statistics screen in Figure 4-5-7 appears.

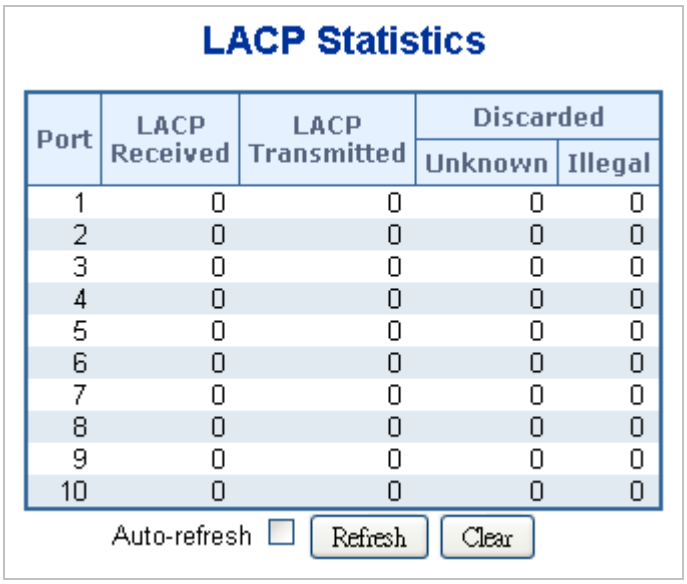


Figure 4-5-7: LACP Statistics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number.
• **LACP Received**	Shows how many LACP frames have been sent from each port.
• **LACP Transmitted**	Shows how many LACP frames have been received at each port.
• **Discarded**	Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh : Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

4.6 VLAN

4.6.1 VLAN Overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.
3. The Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

This section has the following items:

VLAN Basic Information	Displays VLAN information
VLAN Port Configuration	Enables VLAN group
VLAN Memberships	Configures the VLAN membership
VLAN Membership Status	Displays VLAN membership status
VLAN Port Status	Displays VLAN port status
Private VLAN	Creates/removes primary or community VLANs
Port Isolation	Enables/disables port isolation on port
MAC-based VLAN	Configures the MAC-based VLAN entries
MAC-based VLAN Status	Displays MAC-based VLAN entries
IP Subnet-based VLAN	Configures the IP Subnet-based VLAN entries
Protocol-based VLAN	Configures the protocol-based VLAN entries
Protocol-based VLAN Membership	Displays the protocol-based VLAN entries

4.6.2 IEEE 802.1Q VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This Managed Switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong

to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This Managed Switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

IEEE 802.1Q Standard

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either **tagging** or **untagging**.:

- The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.
- The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

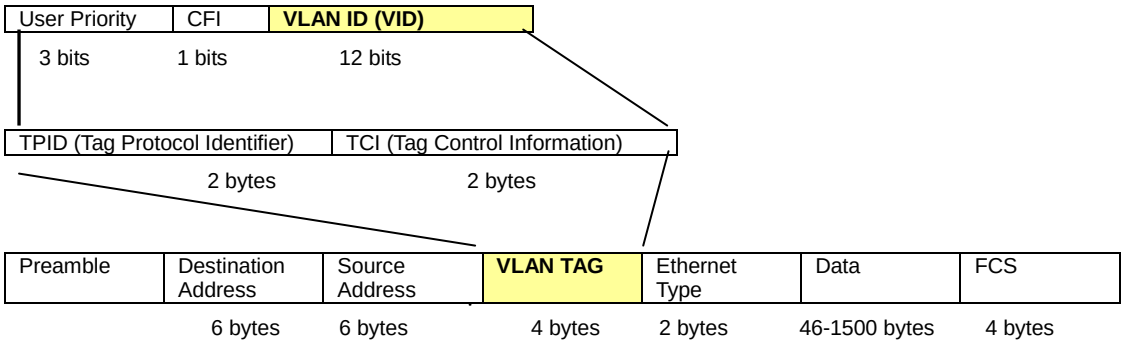
802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of **0x8100** in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet

backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

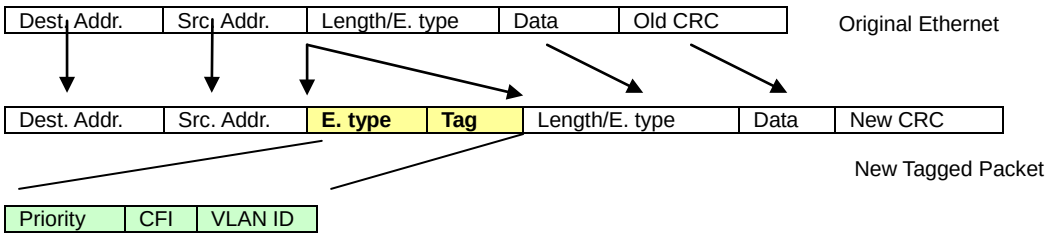
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag



■ Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of

a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called **"default."** The factory default setting assigns all ports on the Switch to the **"default"**. As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices or the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

4.6.3 VLAN Basic Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the Managed Switch.

The VLAN Basic Information screen in Figure 4-6-1 appears.

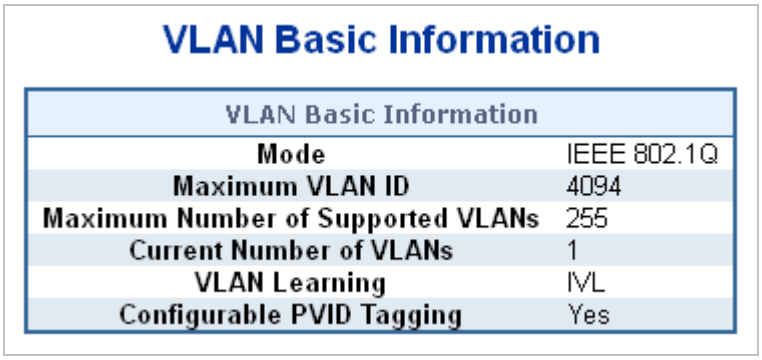


Figure 4-6-1: VLAN Basic Information Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Display the current VLAN mode used by this Managed Switch ■ Port-Based ■ IEEE 802.1Q VLAN
• **Maximum VLAN ID**	Maximum VLAN ID recognized by this Industrial Managed Switch.
• **Maximum Number of Supported VLANs**	Maximum number of VLANs that can be configured on this Industrial Managed Switch.
• **Current number of VLANs**	Display the current number of VLANs
• **VLAN Learning**	Display the VLAN learning mode. The Industrial Managed Switch supports IVL (IVL Independent vlan learning).
• **Configurable PVID Tagging**	Indicates whether or not configurable PVID tagging is implemented.

4.6.4 VLAN Port Configuration

This page is used for configuring the Managed Switch port VLAN. The VLAN per Port Configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Configuration page. All untagged packets arriving to the device are tagged by the ports PVID.

Understand nomenclature of the Switch

IEEE 802.1Q Tagged and Untagged

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

- **Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- **Untagged:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

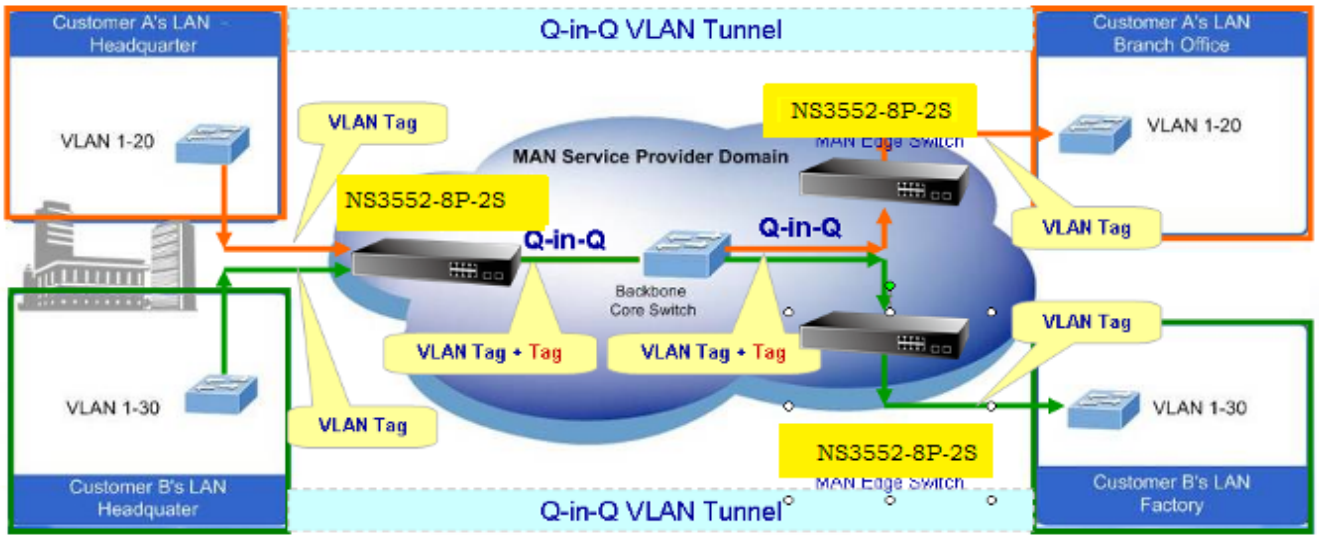
Frame Income / Frame Leave	Income Frame is **tagged**	Income Frame is **untagged**
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

Table 4-6-1 Ingress/Egress port with VLAN VID Tag/Untag table

IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4095.



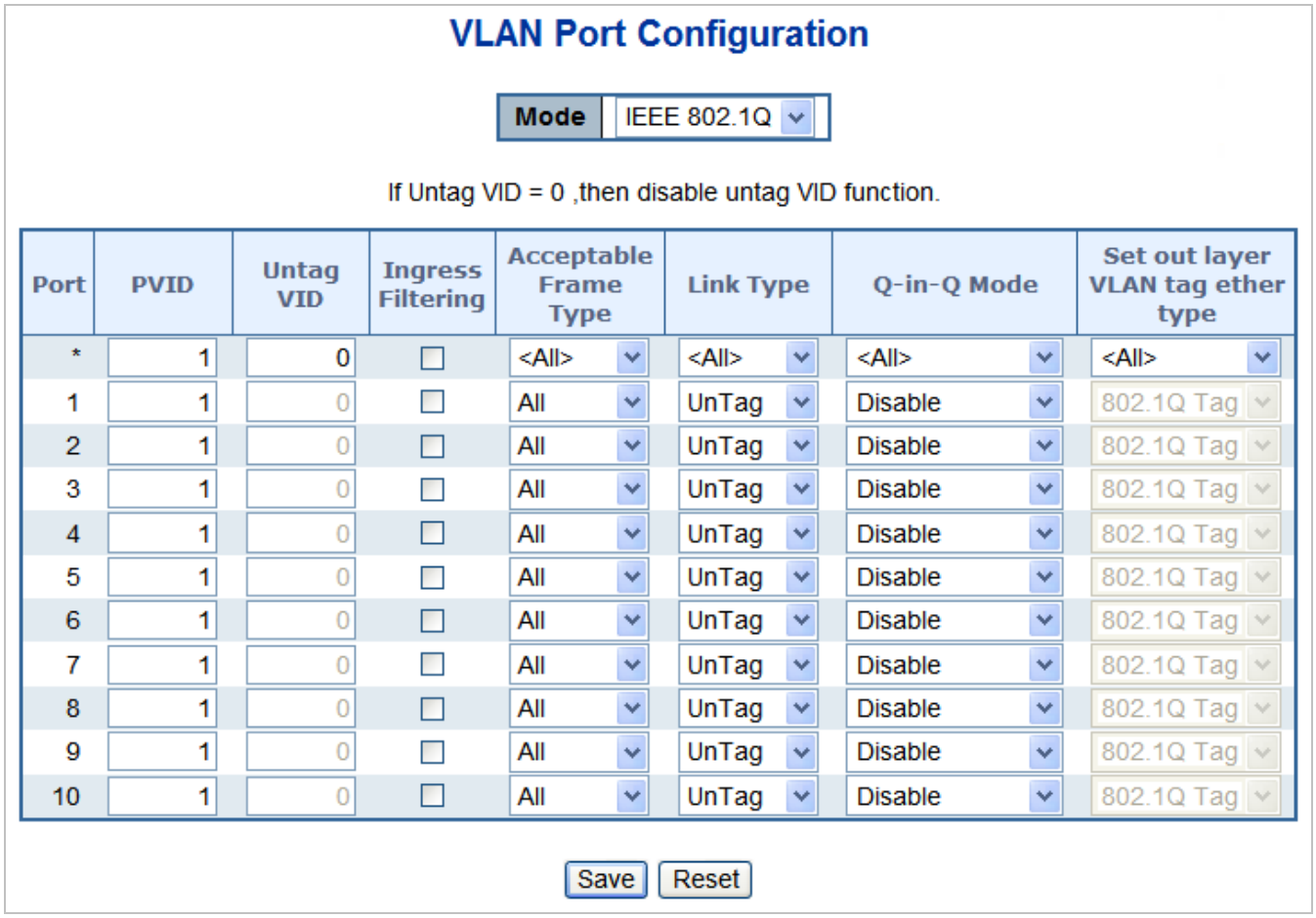
The **Industrial Managed Switch** supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use Ether Type **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

VLAN Port Configuration

The VLAN Port Configuration screen in Figure 4-6-2 appears.



Port	PVID	Untag VID	Ingress Filtering	Acceptable Frame Type	Link Type	Q-in-Q Mode	Set out layer VLAN tag ether type
*	1	0	☐	<All>	<All>	<All>	<All>
1	1	0	☐	All	UnTag	Disable	802.1Q Tag
2	1	0	☐	All	UnTag	Disable	802.1Q Tag
3	1	0	☐	All	UnTag	Disable	802.1Q Tag
4	1	0	☐	All	UnTag	Disable	802.1Q Tag
5	1	0	☐	All	UnTag	Disable	802.1Q Tag
6	1	0	☐	All	UnTag	Disable	802.1Q Tag
7	1	0	☐	All	UnTag	Disable	802.1Q Tag
8	1	0	☐	All	UnTag	Disable	802.1Q Tag
9	1	0	☐	All	UnTag	Disable	802.1Q Tag
10	1	0	☐	All	UnTag	Disable	802.1Q Tag

Figure 4-6-2 : VLAN Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **PVID**	Allows to assign PVID to selected port. The range for the PVID is 1-4094. The PVID will be inserted into all untagged frames entering the ingress port. The PVID must be the same as the VLAN ID in that the port belongs to VLAN group, or the untagged traffic will be dropped.
Untag VID	Allows user to set the port to remove default VID. This option could be edited when Link Type selected to Tagged.
Ingress Filtering	Enable ingress filtering for a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
• **Accept Frame Type**	Determines whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
• **Link Type**	Allow 802.1Q Untagged or Tagged VLAN for selected port. When adding a VLAN to selected port, it tells the switch whether to keep or remove the tag from a frame on egress. ■ **Untag**: outgoing frames without VLAN-Tagged. ■ **Tagged**: outgoing frames with VLAN-Tagged.

• **Q-in-Q Mode**	Sets the Managed Switch to QinQ mode, and allows the QinQ tunnel port to be configured. The default is for the Managed Switch to function in Disable mode. ■ **Disable**: The port operates in its normal VLAN mode. (This is the default.) ■ **MAN Port**: Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network. ■ **Customer Port**: Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
Set Out layer VLAN tag ether type	The Tag Protocol Identifier (TPID) specifies the ether type of incoming packets on a tunnel access port. ■ **802.1Q Tag**: 8100 ■ **vMAN Tag**: 88A8 Default : 802.1Q Tag

The port must be a member of the same VLAN as the Port VLAN ID.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.6.5 VLAN Membership

■ **Adding Static Members to VLANs (VLAN Index)**

Use the VLAN Static Table to configure port members for the selected VLAN index. The VLAN membership configuration for the selected stack switch / unit switch can be monitored and modified here. Up to 255 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN. The VLAN Membership screen in Figure 4-6-3 appears.

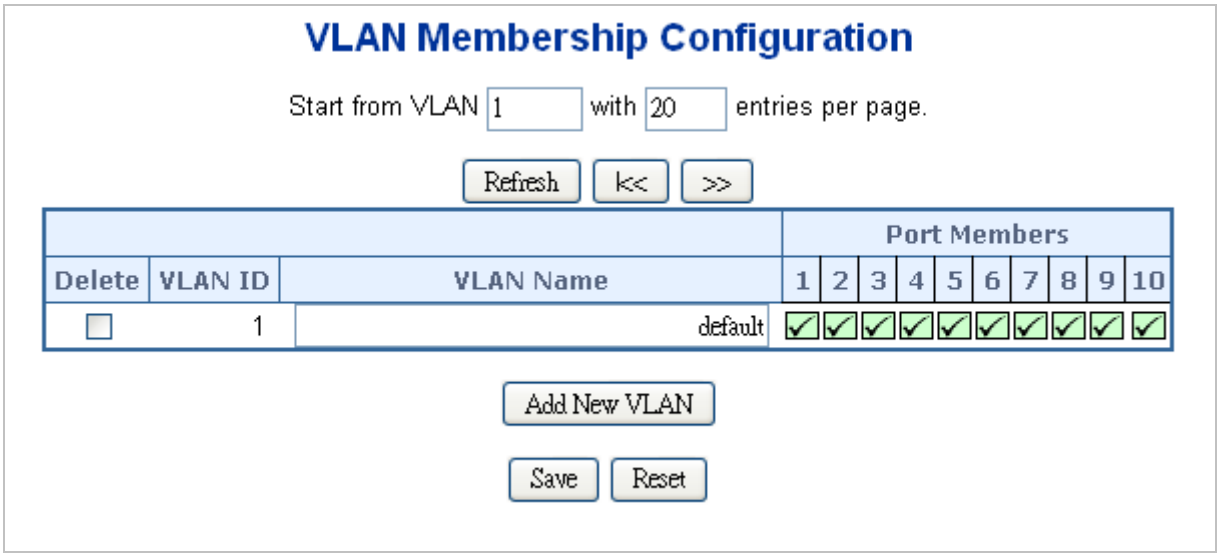


Figure 4-6-3: VLAN Membership Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a VLAN entry, check this box. The entry will be deleted on all stack switch units during the next Save.
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **VLAN Name**	Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. VLAN Name can only contain alphabets or numbers. VLAN name should contain at least one alphabet. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.
• **Port Members**	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
• **Add New VLAN**	Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members. A VLAN without any port members on any stack unit will be deleted when you click "Save". The button can be used to undo the addition of new VLANs.

Buttons

: Click to add new VLAN.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Refreshes the displayed table starting from the "VLAN ID" input fields.

<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.6.6 VLAN Membership Status

This page provides an overview of membership status for VLAN users. The VLAN Membership Status screen in Figure 4-6-4 appears.

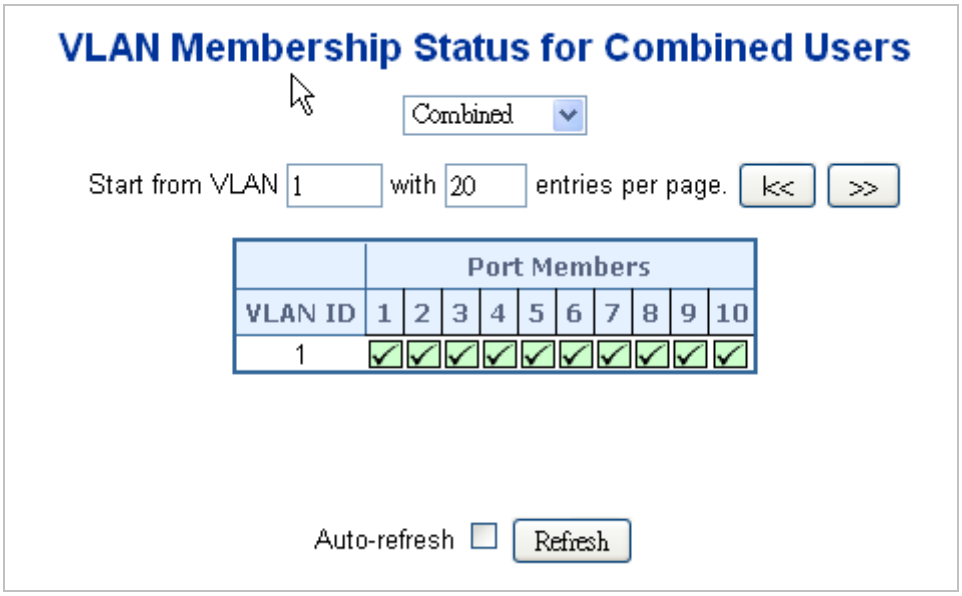


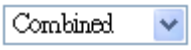
Figure 4-6-4: VLAN Membership Status for Static User Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	Indicates the ID of this particular VLAN.
• **Port Members**	The VLAN Membership Status Page shall show the current VLAN port members for all VLANs configured by a selected VLAN User (selection shall be allowed by a Combo Box). When ALL VLAN Users is selected, it shall show this information for all the VLAN Users, and this is the default. VLAN membership allows the frames Classified to the VLAN ID to be forwarded to the respective VLAN member ports.
• **VLAN User**	A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID and UVID. Currently we support following VLAN : ■ **CLI/Web/SNMP**: This is referred as static. ■ **NAS**: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. ■ **MVR**: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

	■ **Voice VLAN**: Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones. - **MSTP**: The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

Buttons



: Select VLAN Users from this drop down list.

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

: Click to refresh the page immediately.

: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

: Updates the table, starting with the entry after the last entry currently displayed.

4.6.7 VLAN Port Status

This page provides VLAN Port Status. The VLAN Port Status screen in Figure 4-6-5 appears.

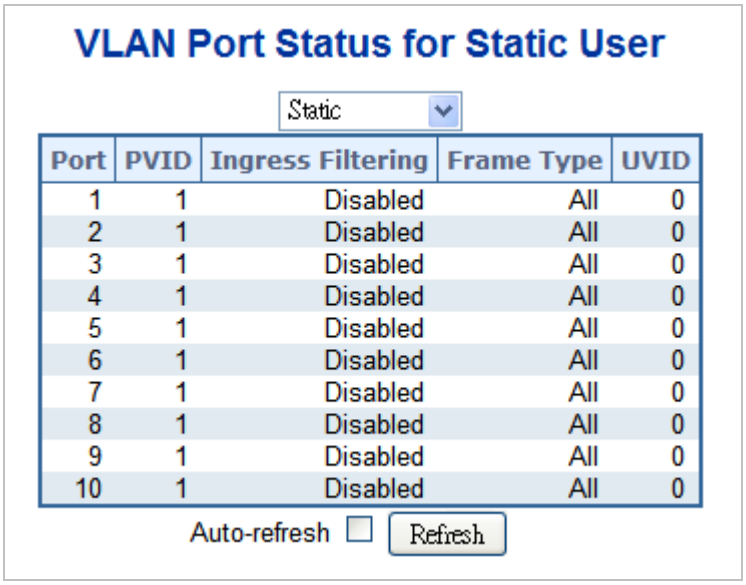

VLAN Port Status for Static User
Static
Port PVID Ingress Filtering Frame Type UVID
1 1 Disabled All 0
2 1 Disabled All 0
3 1 Disabled All 0
4 1 Disabled All 0
5 1 Disabled All 0
6 1 Disabled All 0
7 1 Disabled All 0
8 1 Disabled All 0
9 1 Disabled All 0
10 1 Disabled All 0
Auto-refresh
Refresh

Figure 4-6-5: VLAN Port Status for Static User Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **PVID**	Shows the VLAN identifier for that port. The allowed values are 1 through 4095. The default value is 1.
• **Ingress Filtering**	Shows the ingress filtering for a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded.
• **Frame Type**	Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
• **UVID**	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.

Buttons

Static: Select VLAN Users from this drop down list.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.6.8 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

The Private VLAN screen in Figure 4-6-6 appears.

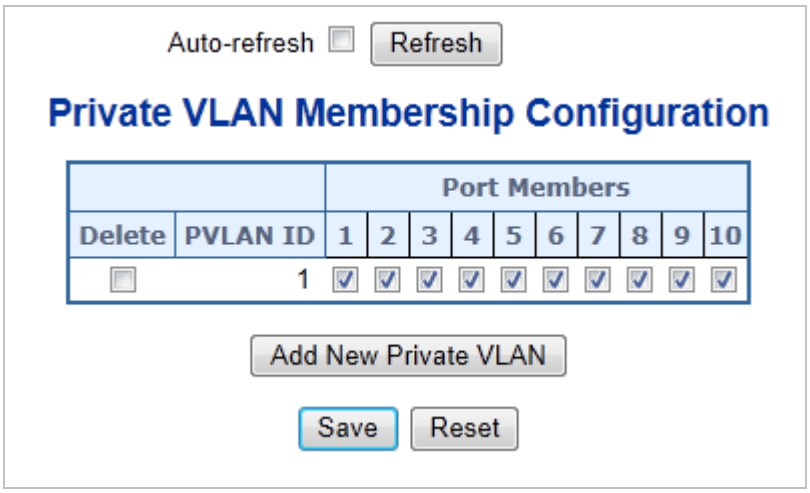


Figure 4-6-6: Private VLAN Membership Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a private VLAN entry, check this box. The entry will be deleted during the next Save.
• **Private VLAN ID**	Indicates the ID of this particular private VLAN.
• **Port Members**	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

Add new Private VLAN: Click to add new VLAN.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

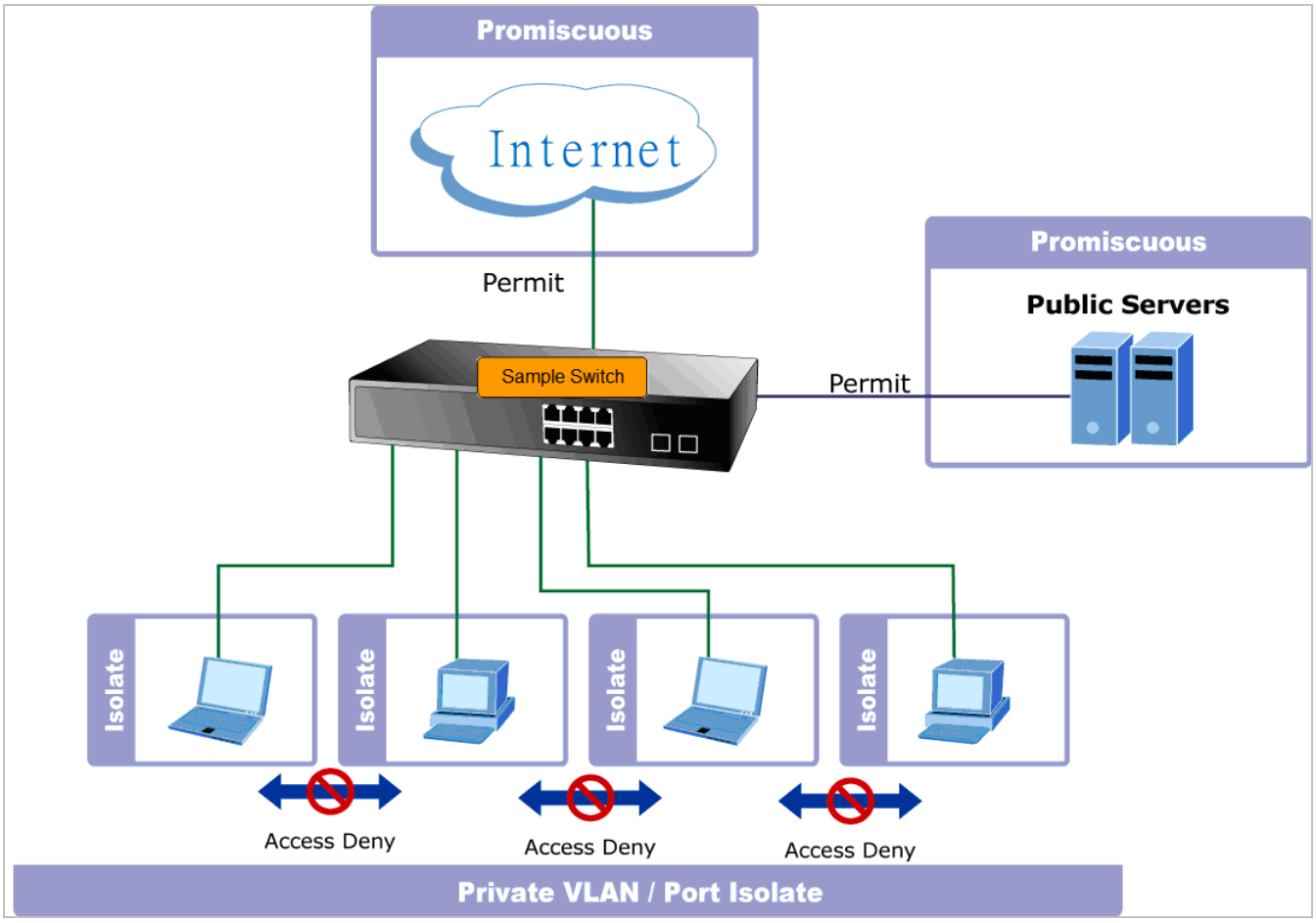
Refresh: Click to refresh the page immediately.

4.6.9 Port Isolation

Overview

When a VLAN is configured to be a private VLAN, communication between ports within that VLAN can be prevented. Two application examples are provided in this section:

- Customers connected to an ISP can be members of the same VLAN, but they are not allowed to communicate with each other within that VLAN.
- Servers in a farm of web servers in a Demilitarized Zone (DMZ) are allowed to communicate with the outside world and with database servers on the inside segment, but are not allowed to communicate with each other



For private VLANs to be applied, the switch must first be configured for standard VLAN operation. When this is in place, one or more of the configured VLANs can be configured as private VLANs. Ports in a private VLAN fall into one of these two groups:

- **Promiscuous ports**
  - — Ports from which traffic can be forwarded to all ports in the private VLAN
  - — Ports which can receive traffic from all ports in the private VLAN

- **Isolated ports**
  - — Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN
  - — Ports which can receive traffic from only promiscuous ports in the private VLAN

The configuration of promiscuous and isolated ports applies to all private VLANs. When traffic comes in on a promiscuous port in a private VLAN, the VLAN mask from the VLAN table is applied. When traffic comes in on an isolated port, the private VLAN mask is applied in addition to the VLAN mask from the VLAN table. This reduces the ports to which forwarding can be done to just the promiscuous ports within the private VLAN.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN. The Port Isolation screen in Figure 4-6-7 appears.

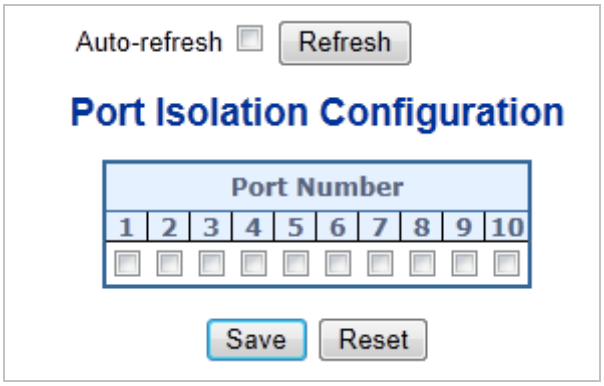


Figure 4-6-7: Port Isolation Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Members**	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.6.10 VLAN Setting Example:

- Separate VLAN
- 802.1Q VLAN Trunk
- Port Isolate

4.6.10.1 Two separate 802.1Q VLAN

The diagram shows how the Industrial Managed Switch handle Tagged and Untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLAN. Each VLAN isolates network traffic so only members of the VLAN receive traffic from the same VLAN members. The screen in Figure 4-6-8 appears and Table 4-1 describes the port configuration of the **Industrial Managed Switch**.

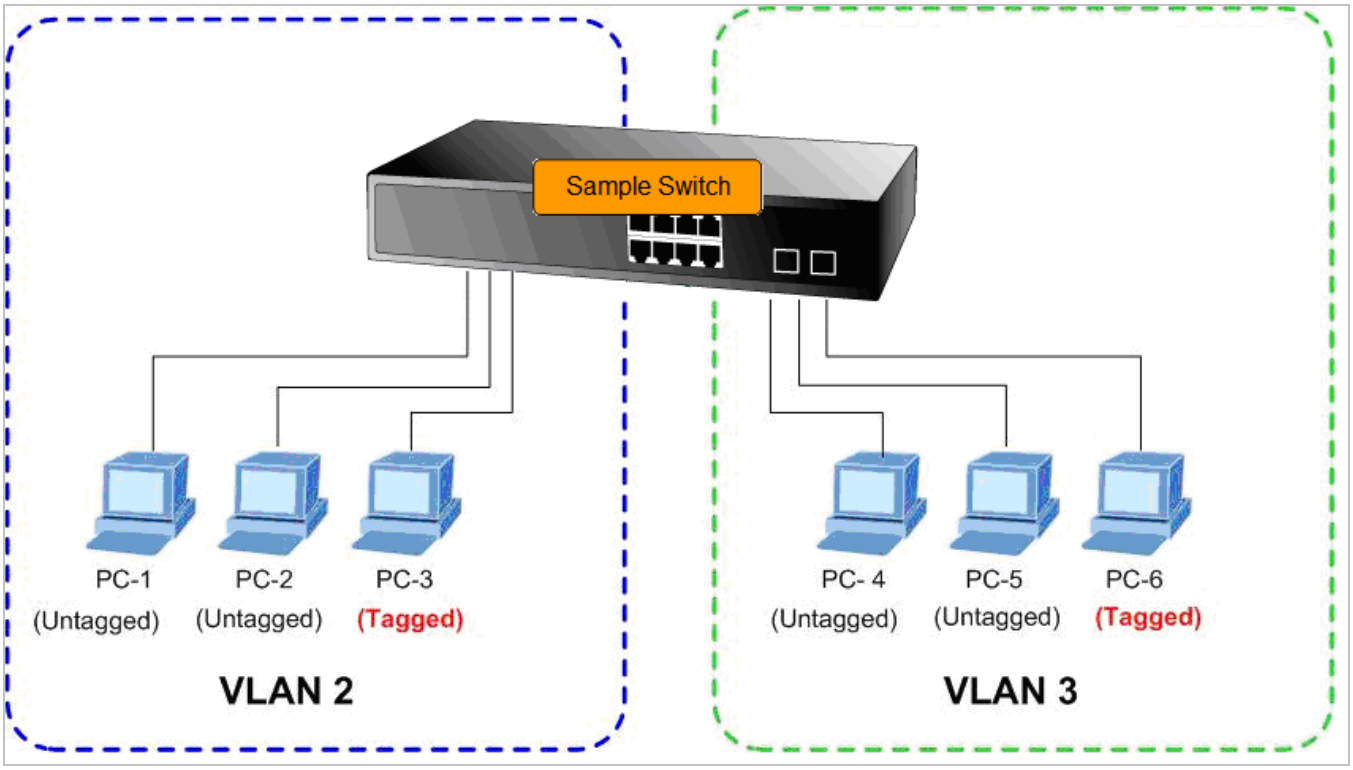


Figure 4-6-8: Two Separate VLAN Diagrams

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7 ~ Port-10	N/A
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6

Table 4-1: VLAN and Port Configuration

The scenario described as follows:

- **Untagged packet entering VLAN 2**

1. While **[PC-1]** transmitting an **untagged** packet enters **Port-1**, the Managed Switch will tag it with a **VLAN Tag=2**. **[PC-2]** and **[PC-3]** will receive the packet through **Port-2** and **Port-3**.
2. [PC-4], [PC-5] and [PC-6] receive no packet.
3. While the packet leaves **Port-2**, it will be stripped away its tag becoming an **untagged** packet.
4. While the packet leaves **Port-3**, it will keep as a **tagged** packet with **VLAN Tag=2**.

■ **Tagged packet entering VLAN 2**

5. While **[PC-3]** transmitting a **tagged** packet with **VLAN Tag=2** enters **Port-3**, **[PC-1]** and **[PC-2]** will receive the packet through **Port-1** and **Port-2**.

6. While the packet leaves **Port-1** and **Port-2**, it will be stripped away its tag becoming an **untagged** packet.

■ **Untagged packet entering VLAN 3**

1. While **[PC-4]** transmitting an **untagged** packet enters **Port-4**, the switch will tag it with a **VLAN Tag=3**. **[PC-5]** and **[PC-6]** will receive the packet through **Port-5** and **Port-6**.

2. While the packet leaves **Port-5**, it will be stripped away its tag becoming an **untagged** packet.

3. While the packet leaves **Port-6**, it will keep as a **tagged** packet with **VLAN Tag=3**.

For this example, just set VLAN Group 1 as default VLAN, but only focus on VLAN 2 and VLAN 3 traffic flow

Setup steps

1. Create VLAN Group

Set VLAN Group 1 = Default-VLAN with VID (VLAN ID) =1

Add two VLANs – VLAN 2 and VLAN 3

VLAN Group 2 with VID=*2*

VLAN Group 3 with VID=*3*

2. Assign VLAN Member :

VLAN 2 : Port-1, Port-2 and Port-3

VLAN 3 : Port-4, Port-5 and Port-6

VLAN 1: All other ports – Port-7~Port-24

3. Remove VLAN Member for VLAN 1:

Remember to remove Port 1 – Port 6 from VLAN 1 membership, since Port 1 – Port 6 has been assigned to VLAN 2 and VLAN 3.

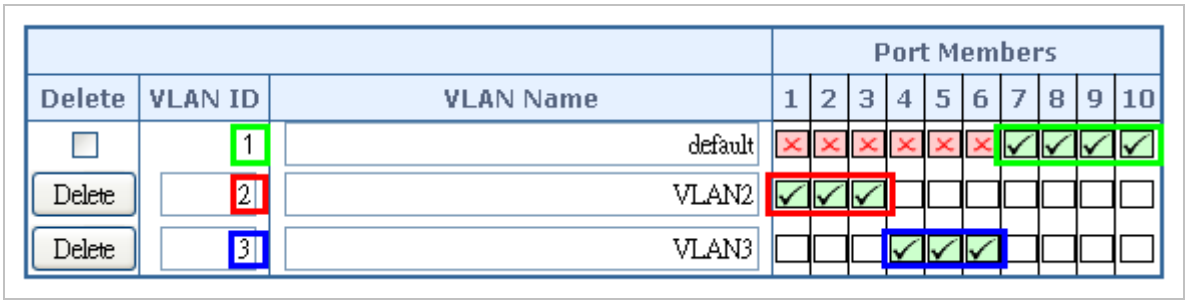


Figure 4-6-9: Add new VLAN group, assign VLAN members to VLAN 2 and VLAN 3 and remove specified ports from VLAN 1 member

It's important to remove the VLAN members from VLAN 1 configuration. Or the ports would become overlap setting. (About the overlapped VLAN configuration, see next VLAN configure sample)

4. Assign PVID to each port:

Port-1, Port-2 and Port-3 : PVID=*2*

Port-4, Port-5 and Port-6 : PVID=*3*

Port-7~Port-24: PVID=*1*

5. Enable VLAN Tag for specific ports

Link Type: *Port-3* (VLAN-2) and *Port-6* (VLAN-3)

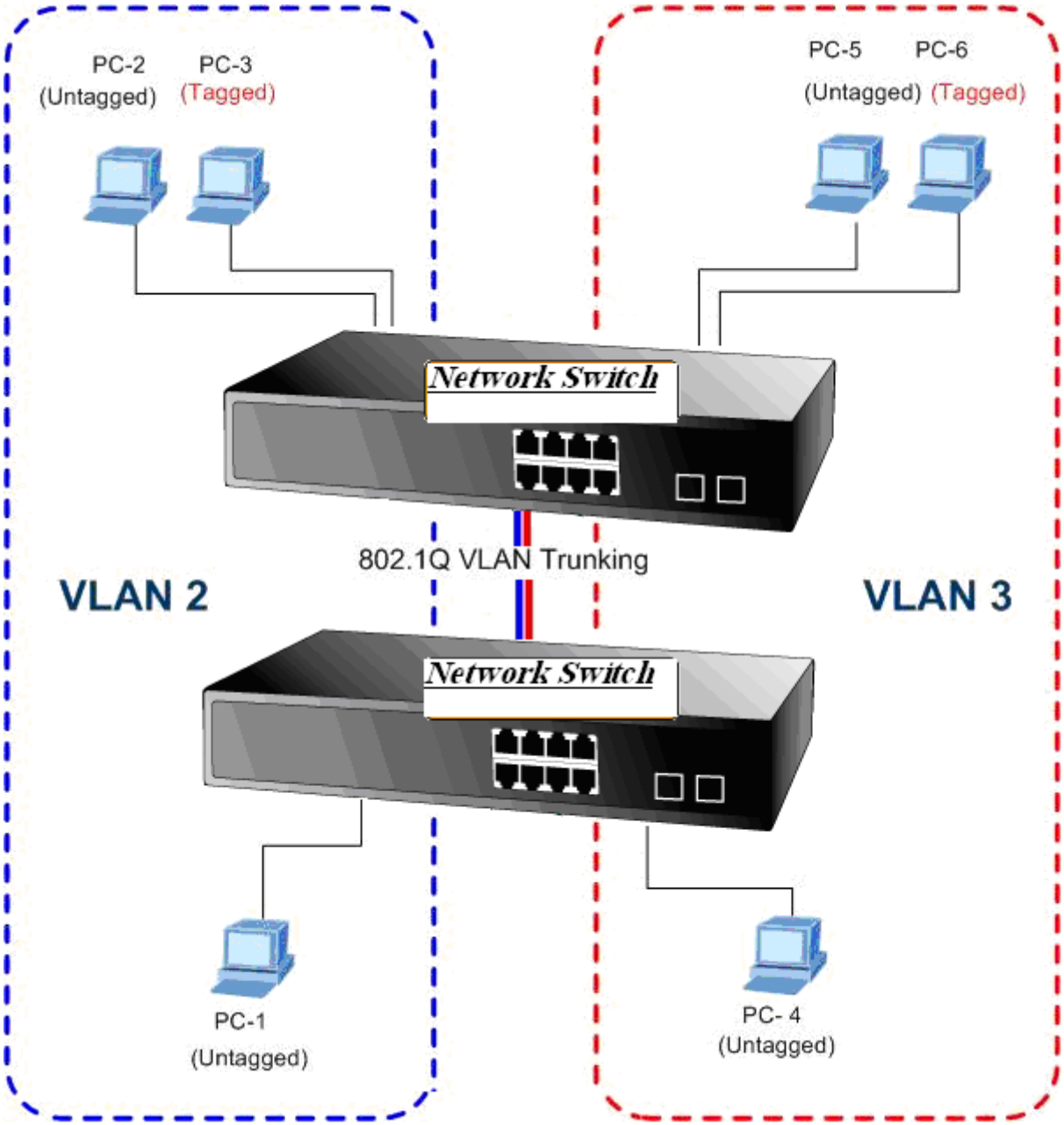
The Per Port VLAN configuration in Figure 4-6-10 appears.

Port	PVID	Ingress Filtering	Acceptable Frame Type	Link Type	Q-in-Q Mode	Set out layer VLAN tag ether type
1	2	☐	All	UnTag	Disable	802.1Q Tag
2	2	☐	All	UnTag	Disable	802.1Q Tag
3	2	☐	All	Tagged	Disable	802.1Q Tag
4	3	☐	All	UnTag	Disable	802.1Q Tag
5	3	☐	All	UnTag	Disable	802.1Q Tag
6	3	☐	All	Tagged	Disable	802.1Q Tag
7	1	☐	All	UnTag	Disable	802.1Q Tag
8	1	☐	All	UnTag	Disable	802.1Q Tag
9	1	☐	All	UnTag	Disable	802.1Q Tag
10	1	☐	All	UnTag	Disable	802.1Q Tag

Figure 4-6-10: Port 1-Port 6 VLAN Configurations

4.6.10.2 VLAN Trunking between two 802.1Q aware Switch

In most cases, it is used for "**Uplink**" to other switches. VLANs are separated at different switches, but they need to access with other switches within the same VLAN group. The screen in Figure 4-6-11 appears.



Setup steps

1. Create VLAN Group

Set VLAN Group 1 = Default-VLAN with VID (VLAN ID) =1

Add two VLANs – VLAN 2 and VLAN 3

VLAN Group 2 with VID=*2*

VLAN Group 3 with VID=*3*

2. Assign VLAN Member :

VLAN 2 : Port-1, Port-2 and Port-3

VLAN 3 : Port-4, Port-5 and Port-6

VLAN 1: All other ports – Port-7~Port-24

As to the VLAN ports connecting to the hosts, please refer to 4.6.10.1 examples. The following steps will focus on the VLAN **Trunk port** configuration.

1. Specify **Port-8** to be the 802.1Q VLAN **Trunk port**.
2. Assign **Port-8** to both **VLAN 2** and **VLAN 3** at the VLAN Member configuration page.
3. Define a **VLAN 1** as a **"Public Area"** that overlaps with both **VLAN 2 members** and **VLAN 3 members**.
4. Assign the VLAN Trunk Port to be the member of each VLAN, which wants to be aggregated. For this sample, assign **Port-8** to be a **VLAN 2** and **VLAN 3** member port. The screen in Figure 4-6-12 appears.

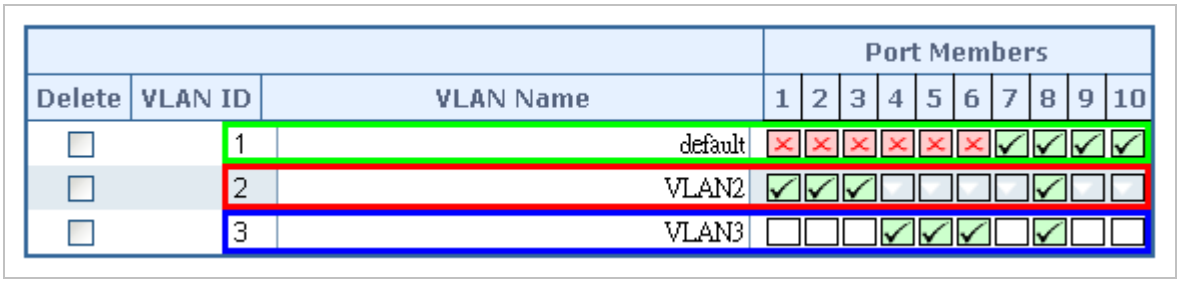


Figure 4-6-12: VLAN overlap port setting & VLAN 1 – The Public Area Member Assign

5. Specify **Port-8** to be the 802.1Q VLAN **Trunk port**, and the Trunking port must be a **Tagged** port while egress. The Port-8 configuration is shown in the following screen in Figure 4-6-13.

Figure 4-6-13: The configuration of VLAN Trunk Port

That is, although the VLAN 2 members: Port-1 to Port-3 and VLAN 3 members: Port-4 to Port-6 also belongs to VLAN 1. But with different PVID settings, packets from VLAN 2 or VLAN 3 are not able to access to the other VLAN.

6. Repeat Steps 1 to 5, set up the VLAN Trunk port at the partner switch and add more VLANs to join the VLAN trunk. Repeat Steps 1 to 3 to assign the Trunk port to the VLANs.

4.6.10.3 Port Isolate

The diagram shows how the Managed Switch handles isolate and promiscuous ports, and the each PC is not able to access each other PCs of each isolate port. But they all need to access with the same server/AP/Printer. The screen in Figure 4-6-14 appears. This section will show you how to configure the port for the server – that could be accessed by each isolate port.

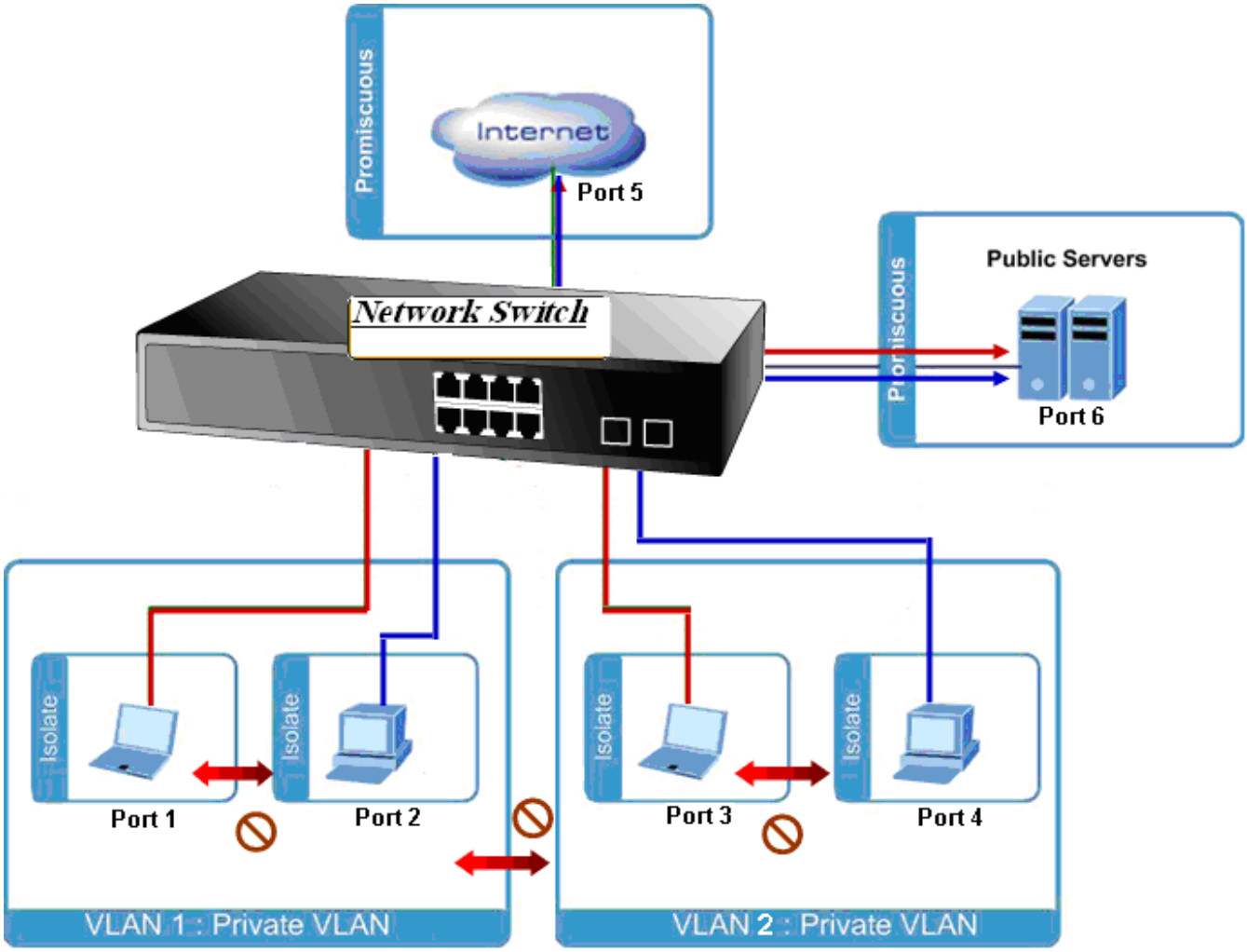


Figure 4-6-14: The Port Isolate VLAN Diagram

Setup steps

1. Assign Port Mode

Set Port-1~Port-4 in Isolate port.

Set Port5 and Port-6 are in Promiscuous port. The screen in Figure 4-6-15 appears.

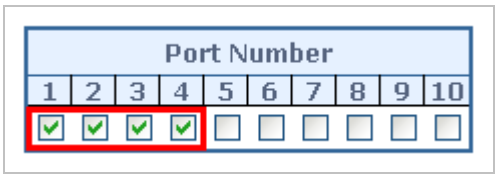


Figure 4-6-15: The Configuration of Isolate and Promiscuous Port

2. Assign VLAN Member :

VLAN 1 : Port-1, Port-2, Port-5 and Port-3

VLAN 2: Port-3~Port-6. The screen in Figure 4-6-16 appears.

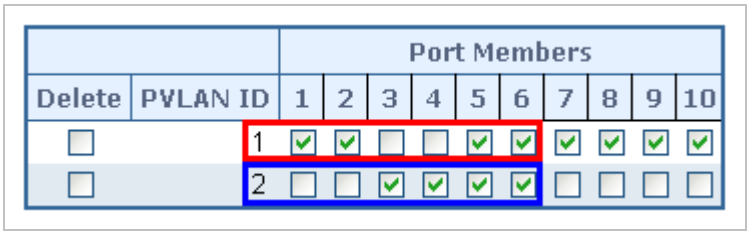


Figure 4-6-16: Private VLAN Port Setting

4.6.11 MAC-based VLAN

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries. The MAC-based VLAN screen in Figure 4-6-17 appears.

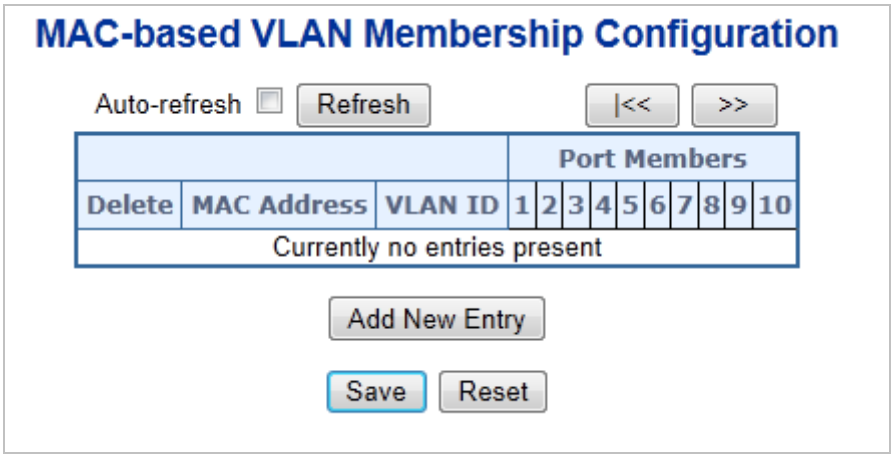


Figure 4-6-17: MAC-based VLAN Membership Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted in the stack.
• **MAC Address**	Indicates the MAC address.
• **VLAN ID**	Indicates the VLAN ID.
• **Port Members**	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

Add new entry: Click to add a new MAC-based VLAN entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<< : Updates the table starting from the first entry in the MAC-based VLAN Table.

>> : Updates the table, starting with the entry after the last entry currently displayed.

4.6.12 MAC-based VLAN Status

This page shows MAC-based VLAN entries configured by various MAC-based VLAN users. The MAC-based VLAN Status screen in Figure 4-6-18 appears.

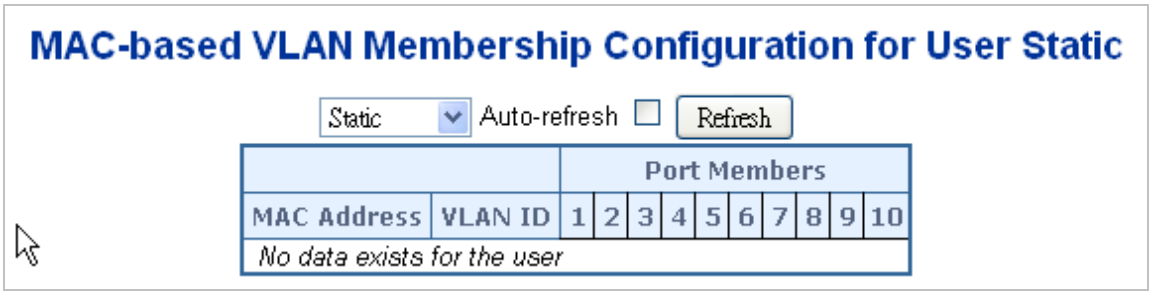


Figure 4-6-18: MAC-based VLAN Membership Configuration for User Static Page Screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	Indicates the MAC address.
• **VLAN ID**	Indicates the VLAN ID.
• **Port Members**	Port members of the MAC-based VLAN entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.6.13 Protocol-based VLAN

This page allows you to add new protocols to Group Name (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the switch. The Protocol-based VLAN screen in Figure 4-6-19 appears.

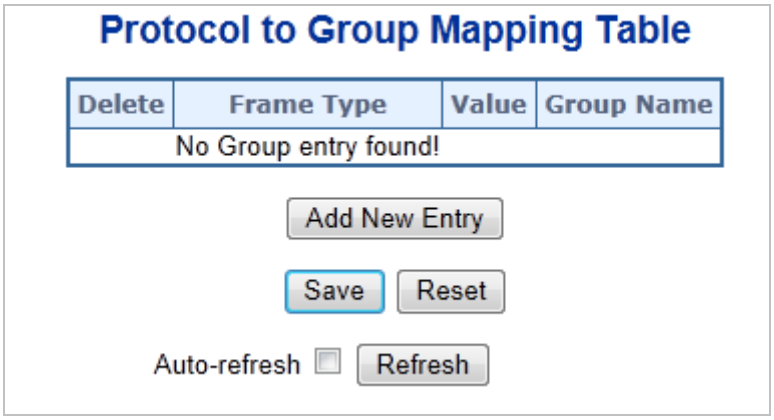


Figure 4-6-19: Protocol to Group Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted on the switch during the next Save.
• **Frame Type**	Frame Type can have one of the following values: 1. **Ethernet** 2. **LLC** 3. **SNAP** Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you select.
• **Value**	Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below is the criteria for three different Frame Types: 1. **For Ethernet**: Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff 2. **For LLC**: Valid value in this case is comprised of two different sub-values. a. **DSAP**: 1-byte long string (0x00-0xff) b. **SSAP**: 1-byte long string (0x00-0xff) 3. **For SNAP**: Valid value in this case also is comprised of two different sub-values. a.**OUI**: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. **PID**: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.
• **Group Name**	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). Note: special character and underscore (_) are not allowed.

Buttons

Add New Entry: Click to add a new entry in mapping table.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.6.14 Protocol-based VLAN Membership

This page allows you to map an already configured Group Name to a VLAN for the switch. The Group Name to VLAN Mapping Table screen in Figure 4-6-20 appears.

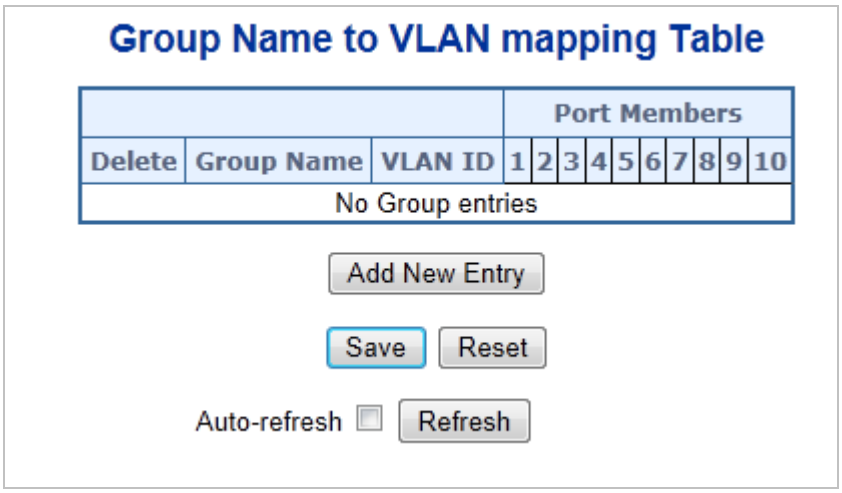


Figure 4-6-20: Group Name to VLAN Mapping Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save
• **Group Name**	A valid Group Name is a string of almost 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers (0-9), no special character is allowed. Whichever Group name you try mapping to a VLAN must be present in Protocol to Group mapping table and must not be preused by any other existing mapping entry on this page.
• **VLAN ID**	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
• **Port Members**	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Buttons

Add New Entry: Click to add a new entry in mapping table.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.7 Spanning Tree Protocol

4.7.1 Theory

The Spanning Tree protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- **STP – Spanning Tree Protocol (IEEE 802.1D)**
- **RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)**
- **MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)**

The **IEEE 802.1D Spanning Tree** Protocol and **IEEE 802.1w Rapid Spanning Tree** Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicated links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port

- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- **Blocking** – the port is blocked from forwarding or receiving packets
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- **□□Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets
- **Forwarding** – the port is forwarding packets
- **Disabled** – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

- From disabled to blocking

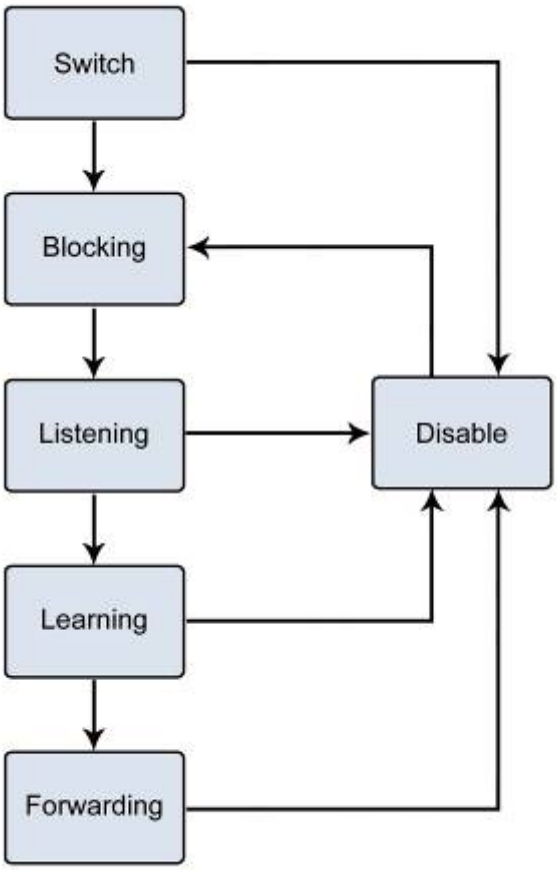


Figure 4-7-1: STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

2. STP Parameters

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.
On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-Changeable STA Parameters

The switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max. Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

Observe the following formulas when setting the above parameters:
Max. Age _ 2 x (Forward Delay - 1 second)
Max. Age _ 2 x (Hello Time + 1 second)

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

3. Illustration of STP

A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.

If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings.

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

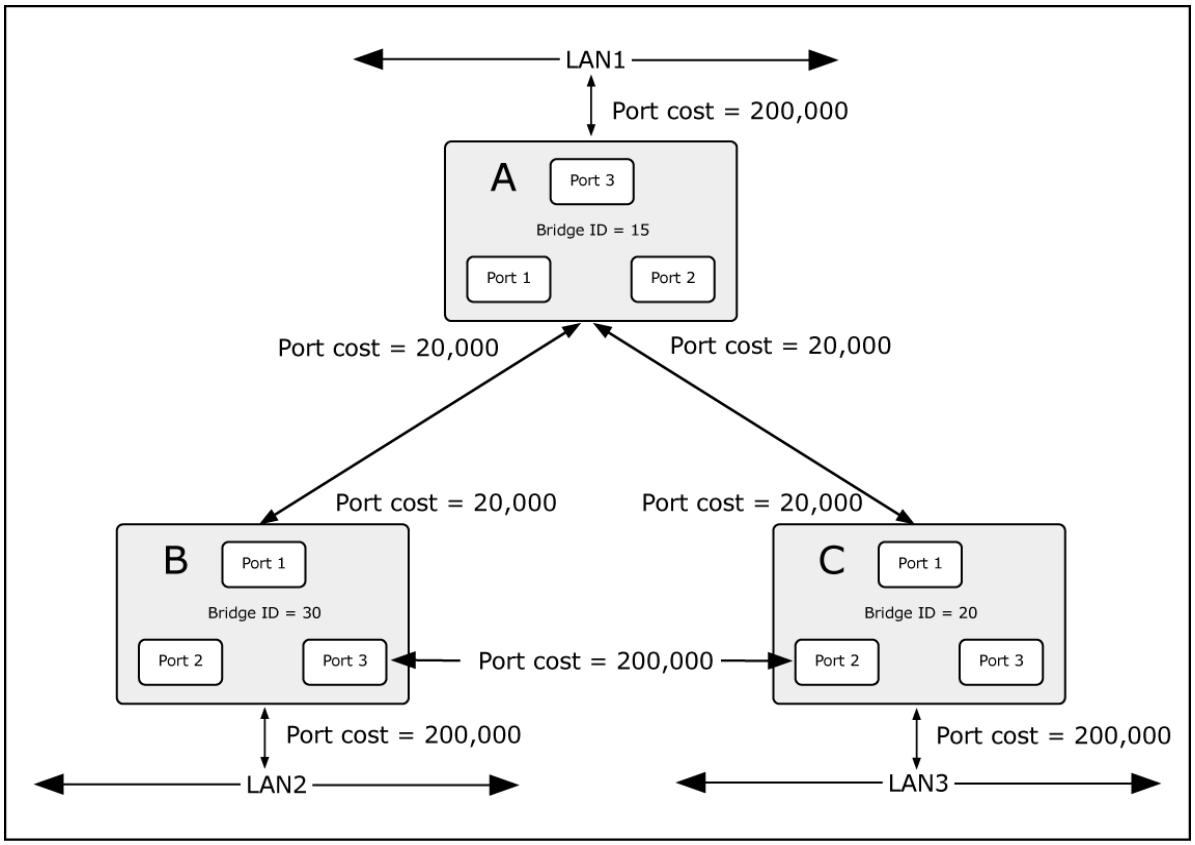


Figure 4-7-2: Before Applying the STA Rules

In this example, only the default STP values are used.

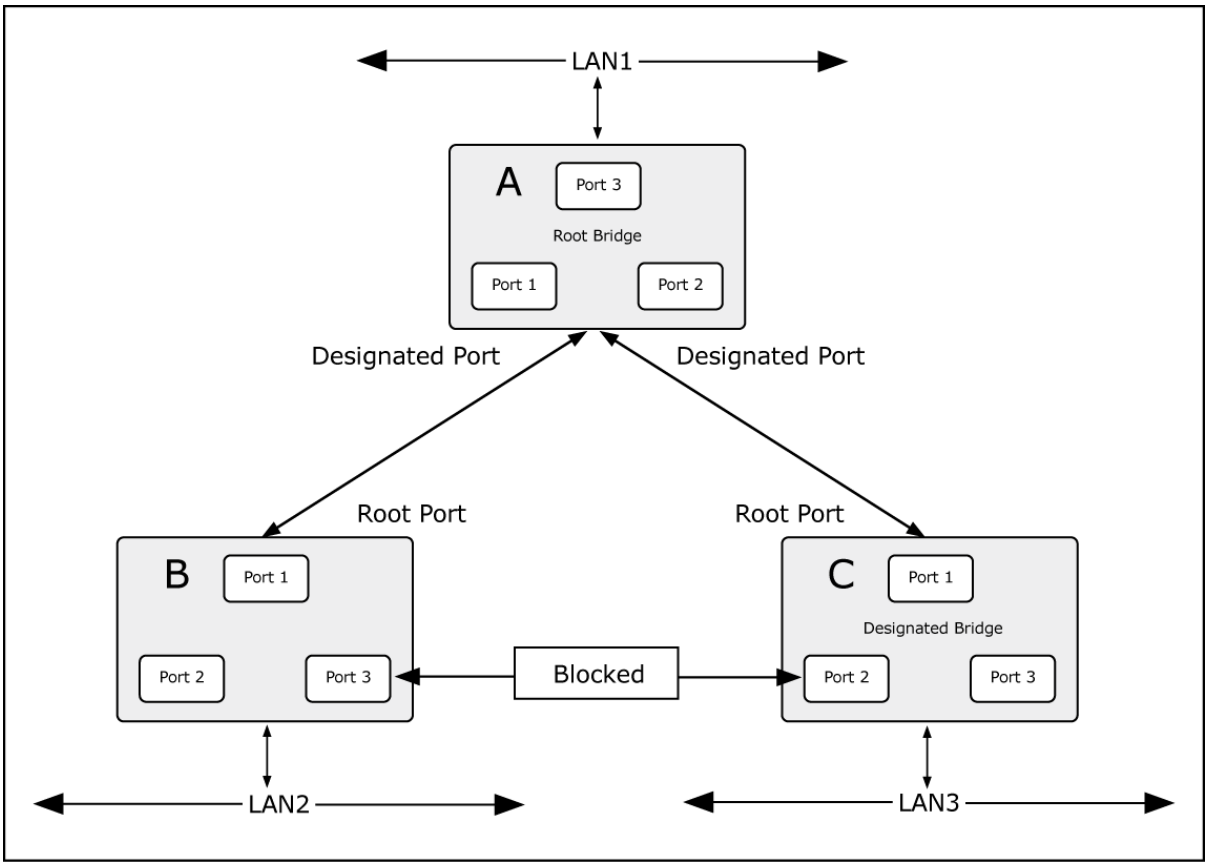


Figure 4-7-3: After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

4.7.2 STP System Configuration

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch or switch Stack. The Managed Switch support the following Spanning Tree protocols:

- **Compatible -- Spanning Tree Protocol (STP):** Provides a single path between end stations, avoiding and eliminating loops.
- **Normal -- Rapid Spanning Tree Protocol (RSTP) :** Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.
- **Extension – Multiple Spanning Tree Protocol (MSTP) :** Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

The STP System Configuration screen in Figure 4-7-4 appears.

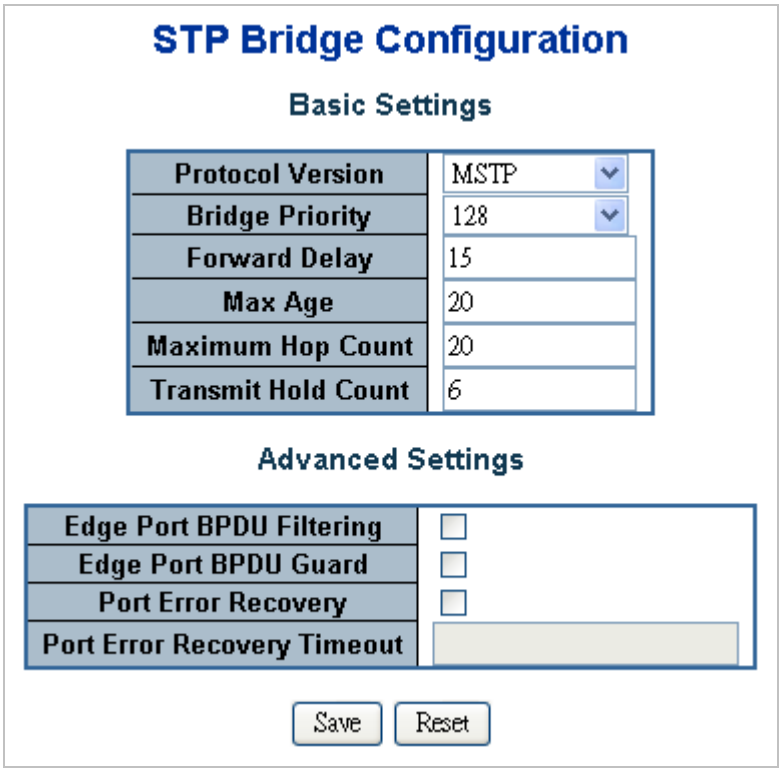


Figure 4-7-4: STP Bridge Configuration Page Screenshot

The page includes the following fields:

Basic Settings

Object	Description
• **Protocol Version**	The STP protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**.
• **Bridge Priority**	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
• **Forward Delay**	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds -Default: 15 -Minimum: The higher of 4 or [(Max. Message Age / 2) + 1] -Maximum: 30
• **Max Age**	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds. -Default: 20 -Minimum: The higher of 6 or [2 x (Hello Time + 1)]. -Maximum: The lower of 40 or [2 x (Forward Delay -1)]
• **Maximum Hop Count**	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 6 to 40 hops.
• **Transmit Hold Count**	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

Object	Description
• **Edge Port BPDU Filtering**	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
• **Edge Port BPDU Guard**	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
• **Port Error Recovery**	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
• **Port Error Recovery Timeout**	The time that has to pass before a port in the *error-disabled* state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

The **Industrial Managed Switch** implements the Rapid Spanning Protocol as the default spanning tree protocol. While selecting **"Compatible"** mode, the system uses the RSTP (802.1w) to be compatible and co work with another STP (802.1D)'s BPDU control packet.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.3 Bridge Status

This page provides a status overview for all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information: The Bridge Status screen in Figure 4-7-5 appears.

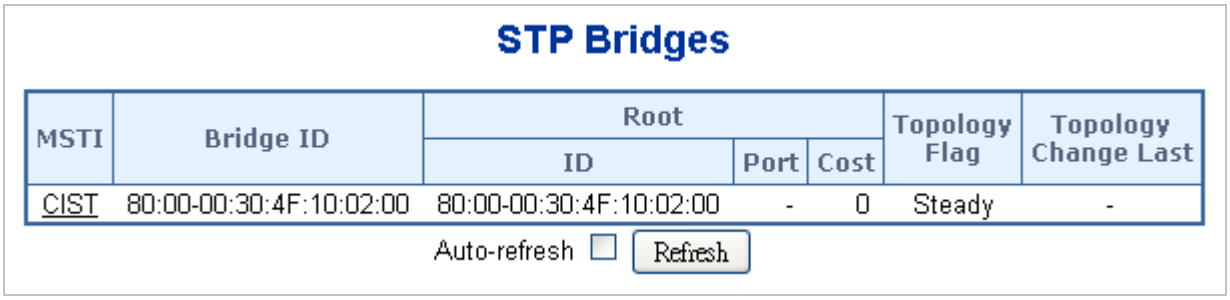


Figure 4-7-5: STP Bridge Status Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI**	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
• **Bridge ID**	The Bridge ID of this Bridge instance.
• **Root ID**	The Bridge ID of the currently elected root bridge.

• **Root Port**	The switch port currently assigned the *root* port role.
• **Root Cost**	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
• **Topology Flag**	The current state of the Topology Change Flag for this Bridge instance.
• **Topology Change Last**	The time since last Topology Change occurred.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.7.4 CIST Port Configuration

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. The CIST Port Configuration screen in Figure 4-7-6 appears.

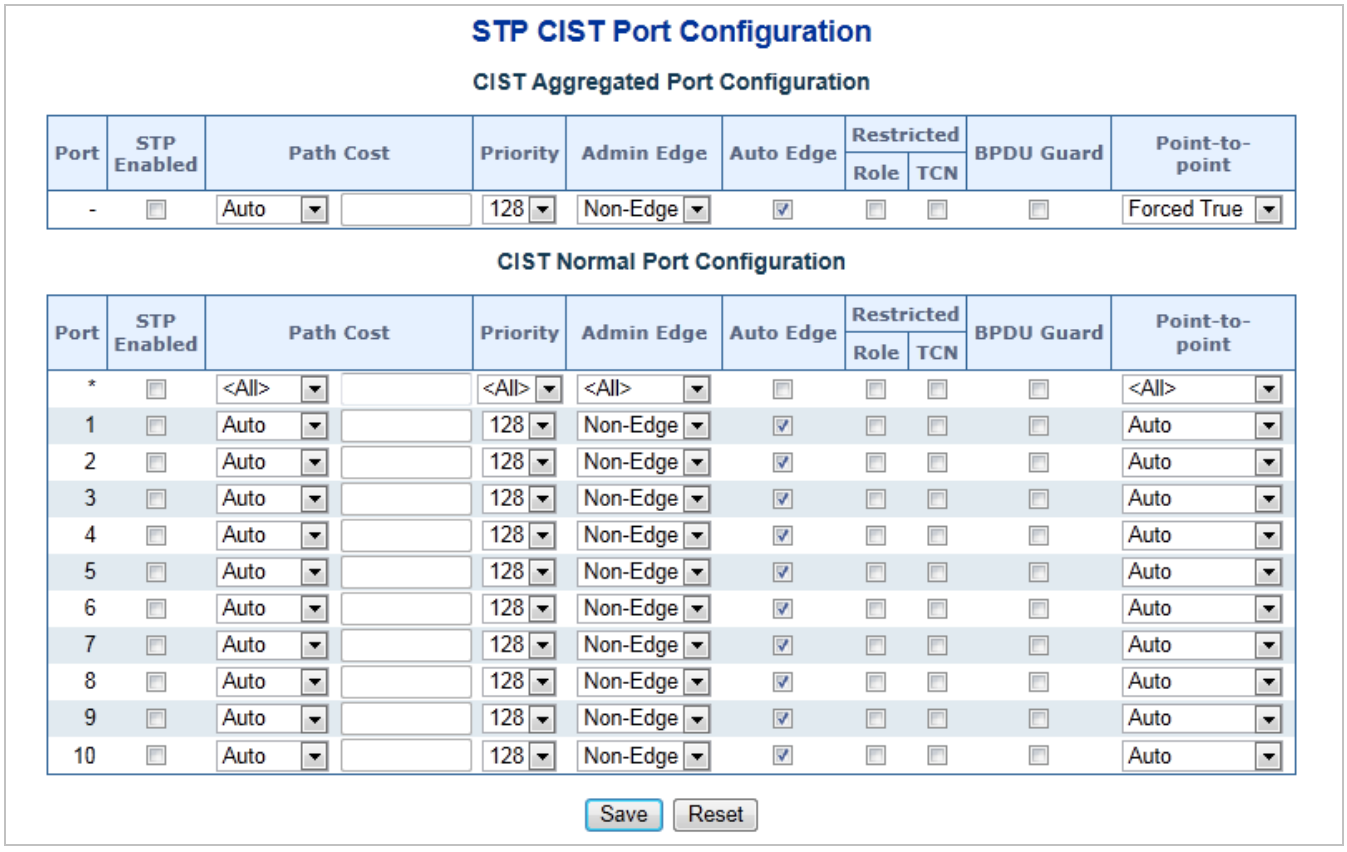


Figure 4-7-6 : STP CIST Port Configuration Page Screenshot

The page includes the following fields:

Object	Description

• **Port**	The switch port number of the logical STP port.
• **STP Enabled**	Controls whether RSTP is enabled on this switch port, * means to select all ports of Industrial Managed Switch.
• **Path Cost**	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. **All** means all ports will have one specific setting.
• **Priority**	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: **128** Range: 0-240, in steps of 16 **All** means all ports will have one specific setting.
• **operEdge (state flag)**	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having *operEdge* true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.
• **Admin Edge**	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized). **All** means all ports will have one specific setting.
• **Auto Edge**	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
• **Restricted Role**	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as **Root Guard**.
• **Restricted TCN**	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
• **BPDU Guard**	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
• **Point-to-Point**	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. A transition to the forwarding state is faster for point-to-point LANs than for shared media. **All** means all ports will have one specific setting.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 802.1w standard exceeds 65,535, the default is set to 65,535.

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000

Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 4-7-1: Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	100 95 90	2,000,000 1,999,999 1,000,000
Fast Ethernet	Half Duplex Full Duplex Trunk	19 18 15	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	4 3	10,000 5,000

Table 4-7-2: Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	2,000,000 1,000,000 500,000
Fast Ethernet	Half Duplex Full Duplex Trunk	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	10,000 5,000

Table 4-7-3: Default STP Path Costs

4.7.5 MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Priority screen in Figure 4-7-7 appears.

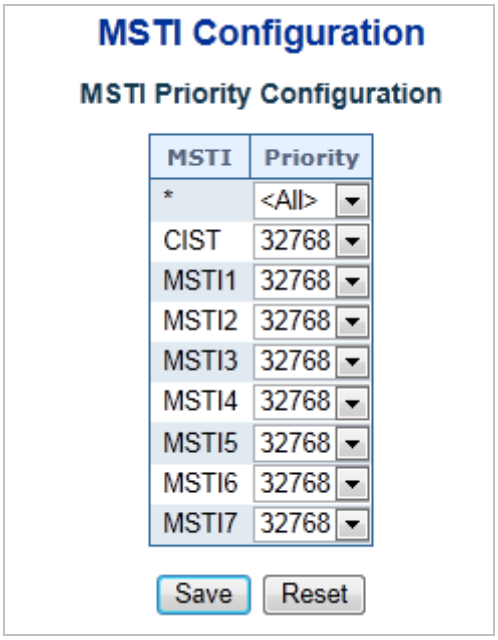


Figure 4-7-7: MSTI Priority Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI**	The bridge instance. The CIST is the default instance, which is always active.
• **Priority**	The Configuration All with available values will assign to whole items. Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier, * means all MSTI items will have one priority setting.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.6 MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The MSTI Configuration screen in Figure 4-7-8 appears.

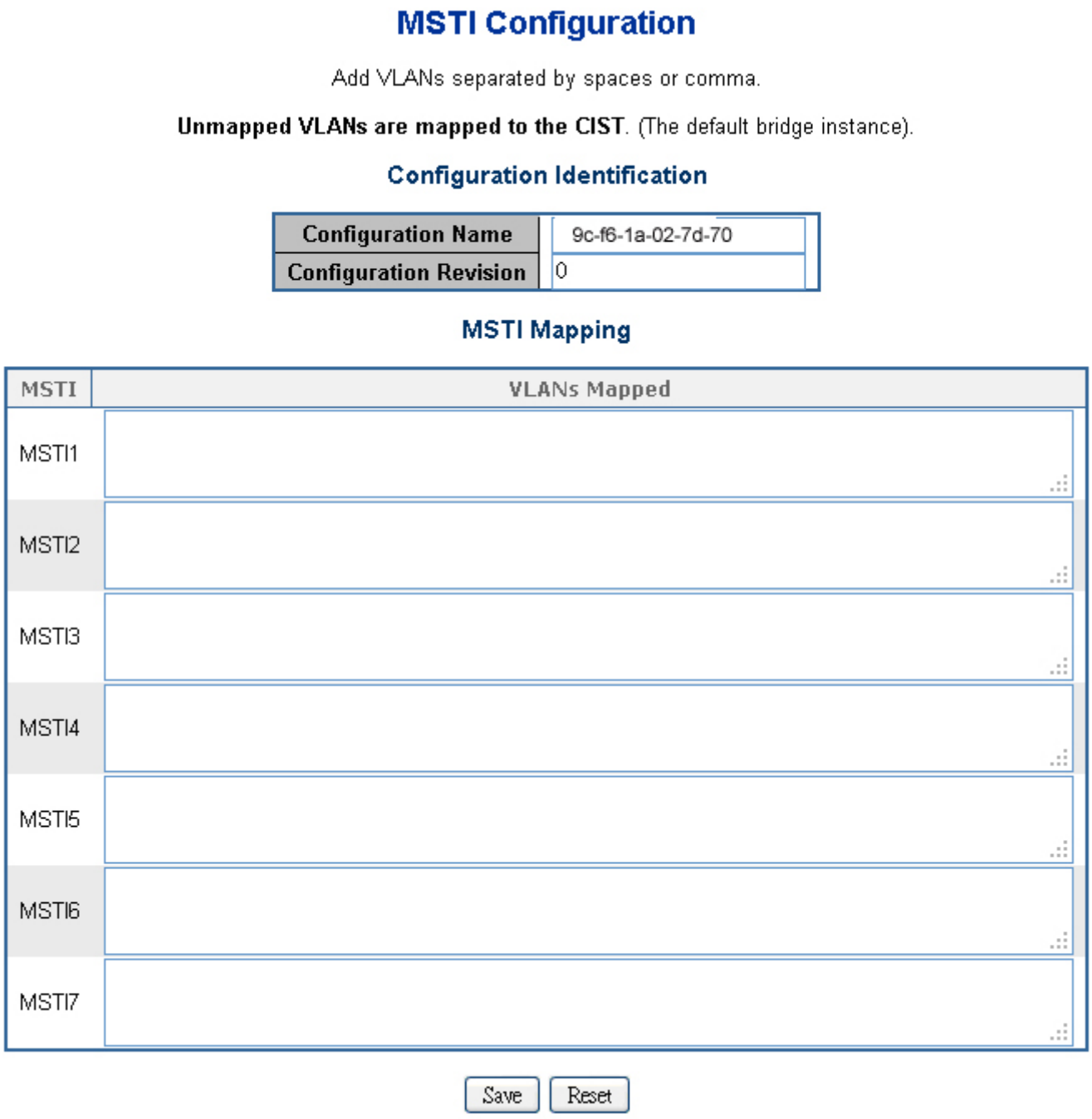


Figure 4-7-8: MSTI Configuration Page Screenshot

The page includes the following fields:

Configuration Identification

Object	Description
• **Configuration Name**	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
• **Configuration Revision**	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

Object	Description
• **MSTI**	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
• **VLANs Mapped**	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. A unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.7 MSTI Ports Configuration

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global. The MSTI Port Configuration screen in Figure 4-7-9 & Figure 4-7-10 appears.

Figure 4-7-9: MSTI Port Configuration Page Screenshot

The page includes the following fields:

MSTI Port Configuration

Object	Description
• **Select MSTI**	Select the bridge instance and set more detail configuration.

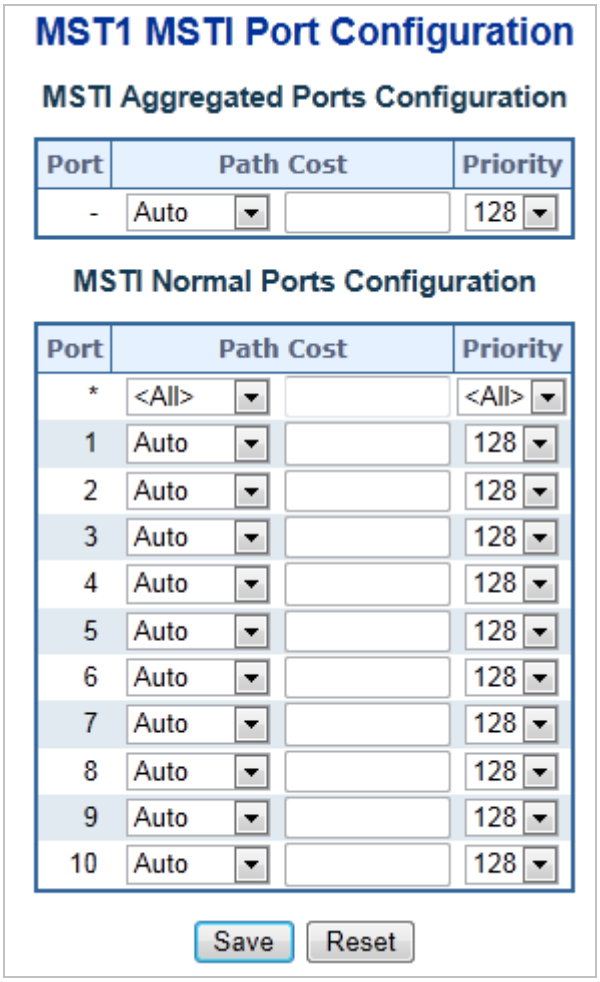


Figure 4-7-10: MST1 MSTI Port Configuration Page Screenshot

The page includes the following fields:

MSTx MSTI Port Configuration

Object	Description
• **Port**	The switch port number of the corresponding STP CIST (and MSTI) port.
• **Path Cost**	The Configuration All with available values will assign to whole items. Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. **All** means all ports will have one specific setting.

• **Priority**	The Configuration All with available values will assign to whole items. Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). **All** means all ports will have one specific setting.

Buttons

Get: Click to set MSTx configuration.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.7.8 Port Status

This page displays the STP CIST port status for port physical ports in the currently selected switch.

The STP Port Status screen in Figure 4-7-11 appears.

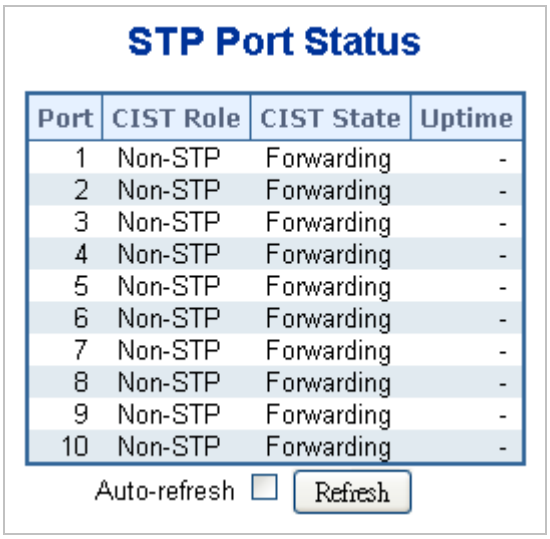


Figure 4-7-11: STP Port Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical STP port.
• **CIST Role**	The current STP port role of the ICST port. The port role can be one of the following values: ■ **AlternatePort** ■ **BackupPort** ■ **RootPort** ■ **DesignatedPort**
• **CIST State**	The current STP port state of the CIST port. The port state can be one of the following values: ■ **Disabled** ■ **Blocking** ■ **Learning** ■ **Forwarding**

	■ **Non-STP**
• **Uptime**	The time since the bridge port was last initialized.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.7.9 Port Statistics

This page displays the STP port statistics counters for port physical ports in the currently selected switch.

The STP Port Statistics screen in Figure 4-7-12 appears.

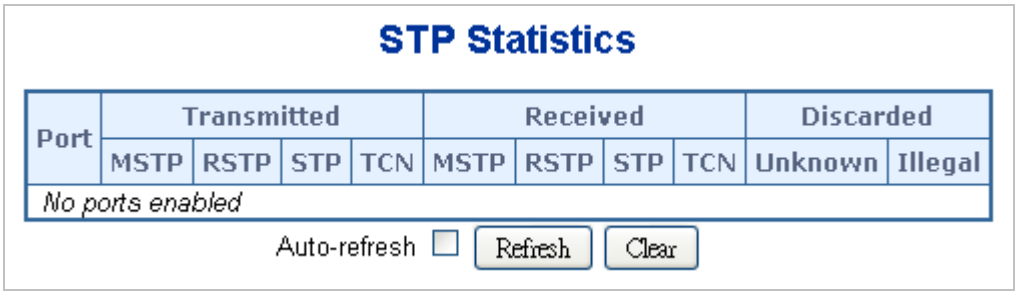


Figure 4-7-12: STP Statistics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical RSTP port.
• **MSTP**	The number of MSTP Configuration BPDU's received/transmitted on the port.
• **RSTP**	The number of RSTP Configuration BPDU's received/transmitted on the port.
• **STP**	The number of legacy STP Configuration BPDU's received/transmitted on the port.
• **TCN**	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
• **Discarded Unknown**	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
• **Discarded Illegal**	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Click to clear the information immediately.

4.8 Multicast

4.8.1 IGMP Snooping

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

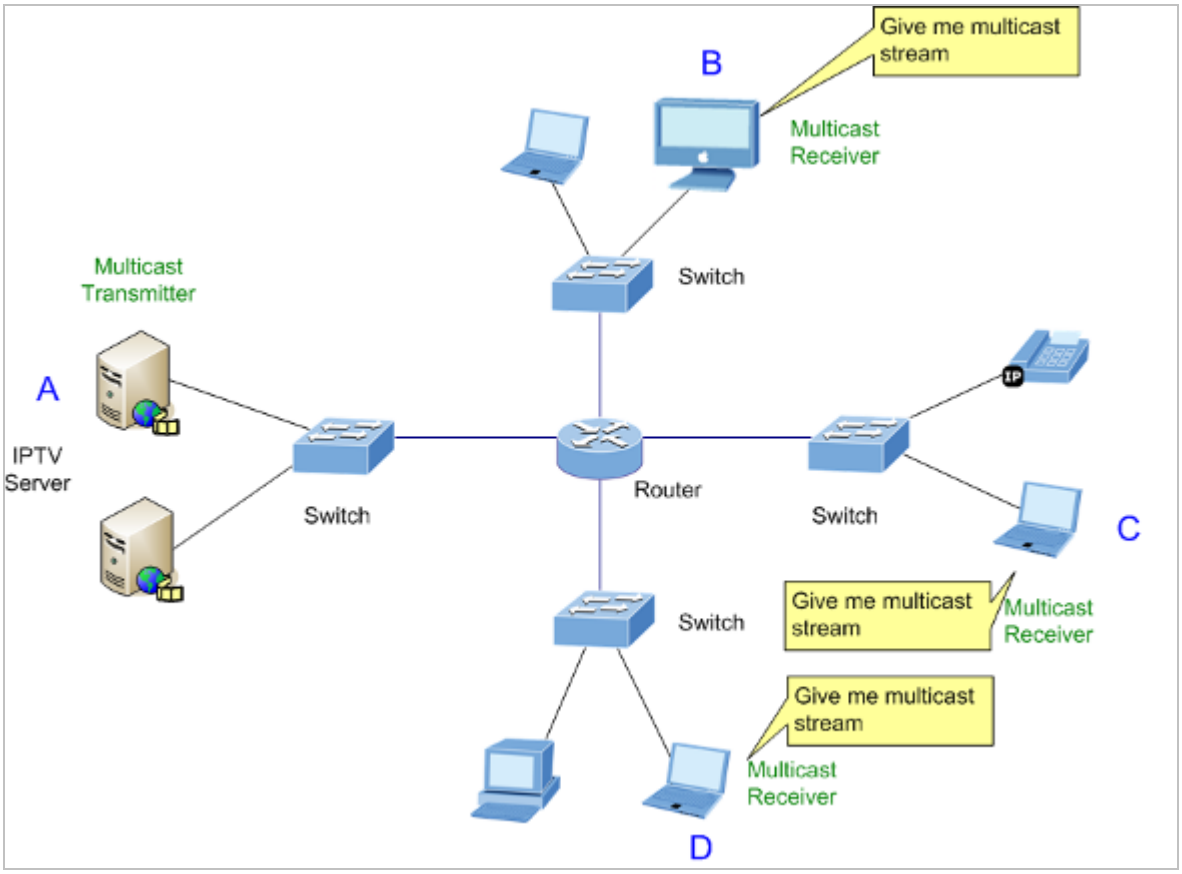


Figure 4-8-1: Multicast Service

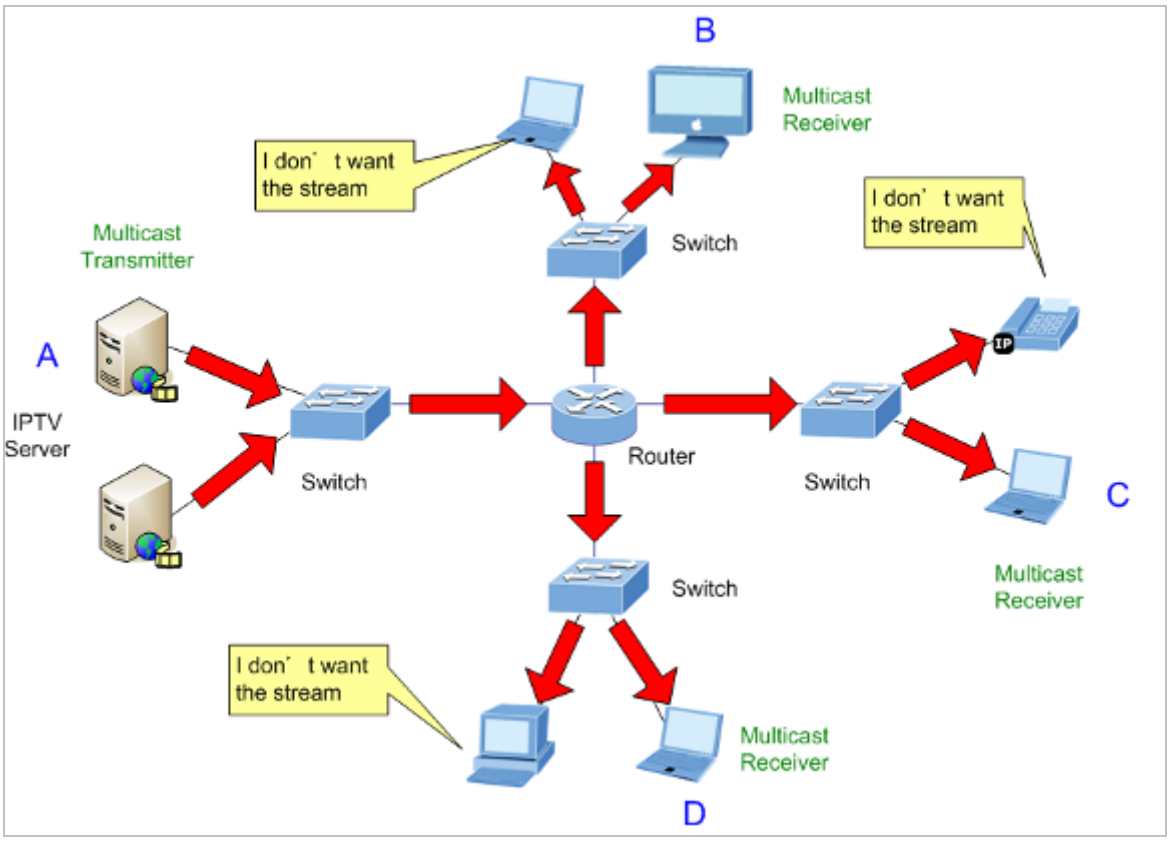


Figure 4-8-2: Multicast Flooding

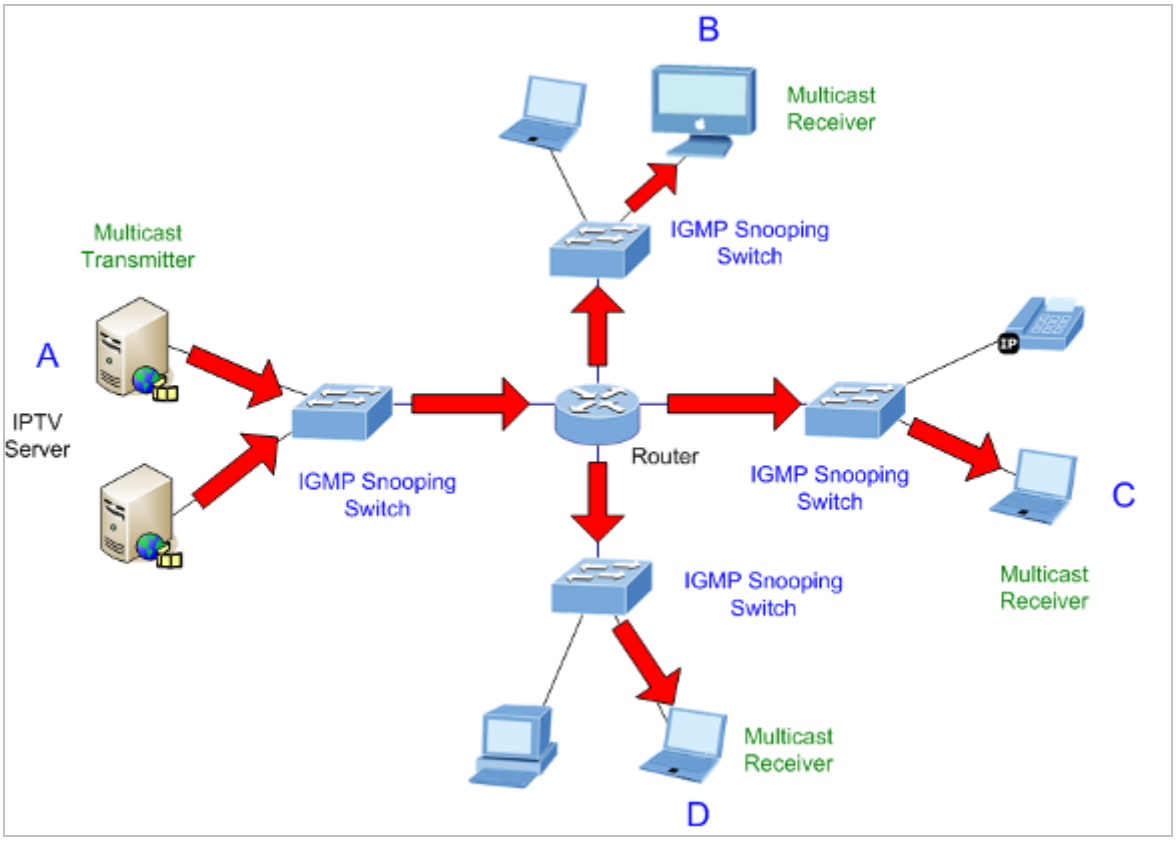


Figure 4-8-3: IGMP Snooping Multicast Stream Control

IGMP Versions 1 and 2

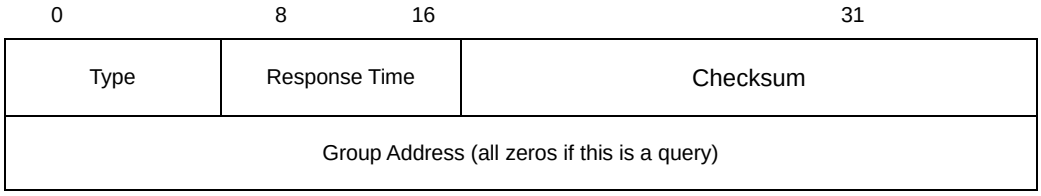
Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets



The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	**Membership Report (version 2)**
0x17	**Leave a Group (version 2)**
0x12	**Membership Report (version 1)**

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

A host sends an IGMP **"report"** to join a group

A host will never send a report when it wants to leave a group (for version 1).

A host will send a **"leave"** report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:

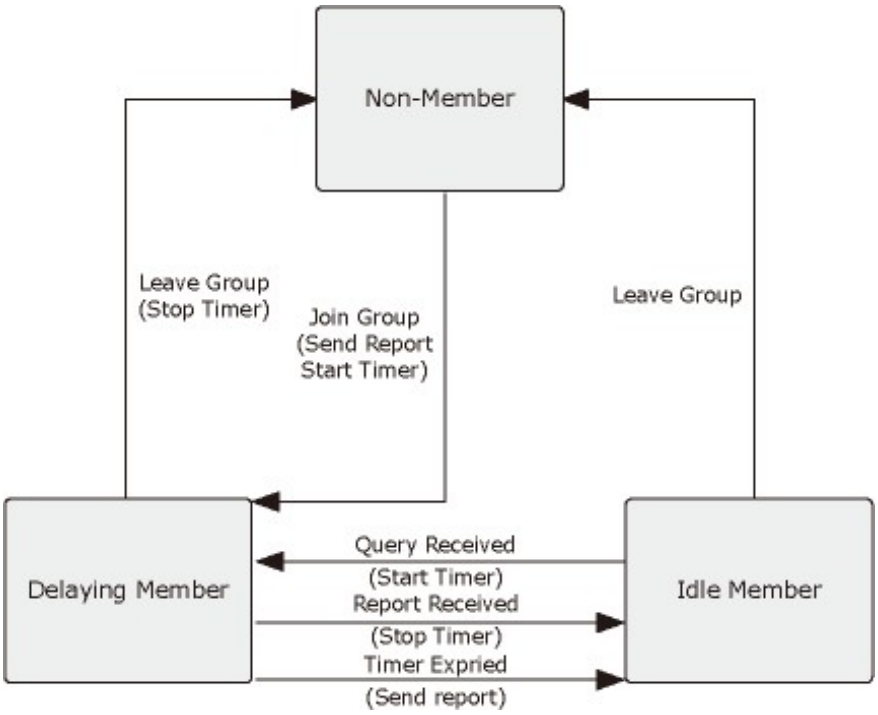


Figure 4-8-4: IGMP State Transitions

- **IGMP Querier –**

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "**querier**" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

4.8.2 IGMP Snooping Configuration

This page provides IGMP Snooping related configuration. The IGMP Snooping Configuration screen in Figure 4-8-5 appears.

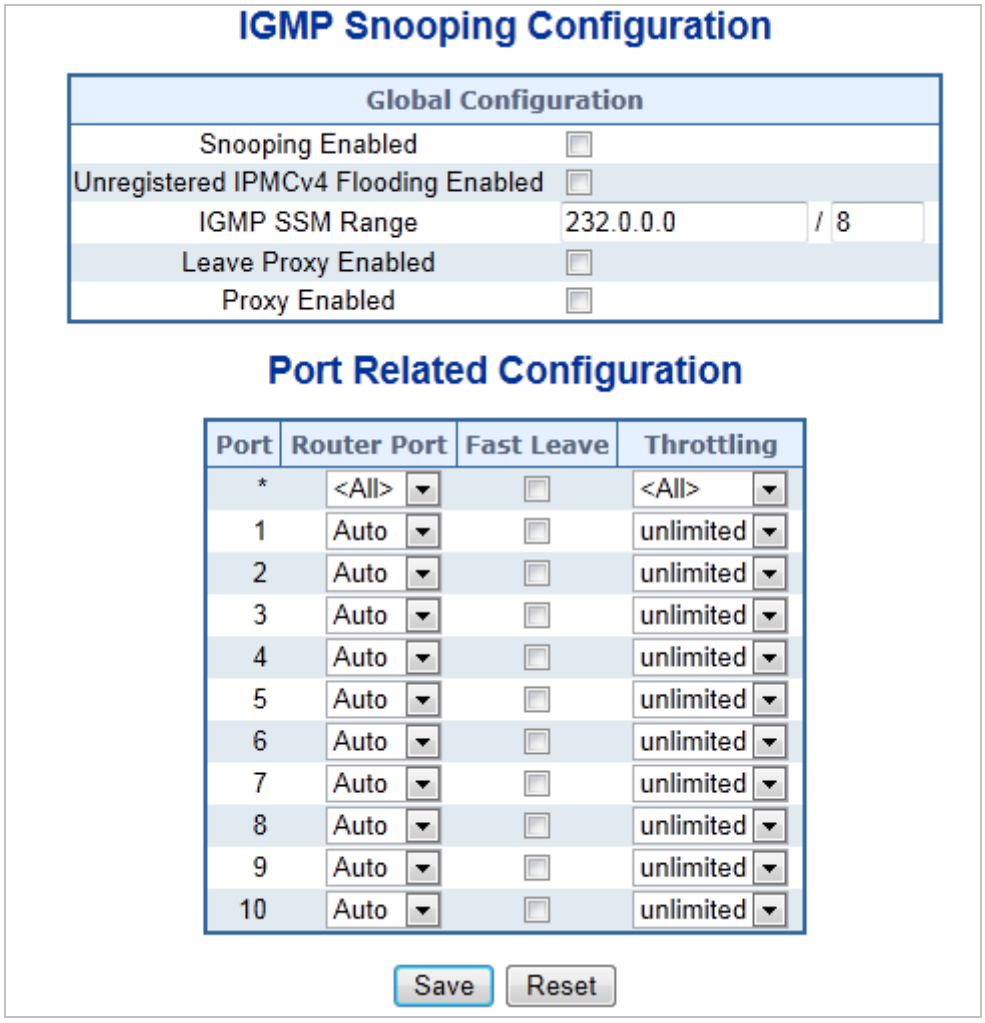


Figure 4-8-5: IGMP Snooping Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Snooping Enabled**	Enable the Global IGMP Snooping.
• **Unregistered IPMCv4 Flooding enabled**	Enable unregistered IPMCv4 traffic flooding.
• **IGMP SSM Range**	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
• **Leave Proxy Enable**	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
• **Proxy Enable**	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
• **Router Port**	Specify which ports act as IGMP router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. The Switch forwards IGMP join or leave packets to an IGMP router port. ■ **Auto:** Select “Auto” to have the Managed Switch automatically uses the port as IGMP Router port if the port receives IGMP query packets.

	■ **Static**: The Managed Switch always uses the specified port as an IGMP Router port. Use this mode when you connect an IGMP multicast server or IP camera which applied with multicast protocol to the port. ■ **None:** The Industrial Managed Switch will not use the specified port as an IGMP Router port. The Managed Switch will not keep any record of an IGMP router being connected to this port. Use this mode when you connect other IGMP multicast servers directly on the non-querier Managed Switch and don't want the multicast stream to be flood to uplink switch through the port that connected to the IGMP querier.
• **Fast Leave**	Enable the fast leave on the port.
• **Throtting**	The Configuration All with available values will assign to whole items. Enable to limit the number of multicast groups to which a switch port can belong. **All** means all ports will have one specific setting.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.3 IGMP Snooping VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The IGMP Snooping VLAN Configuration screen in Figure 4-8-6 appears.

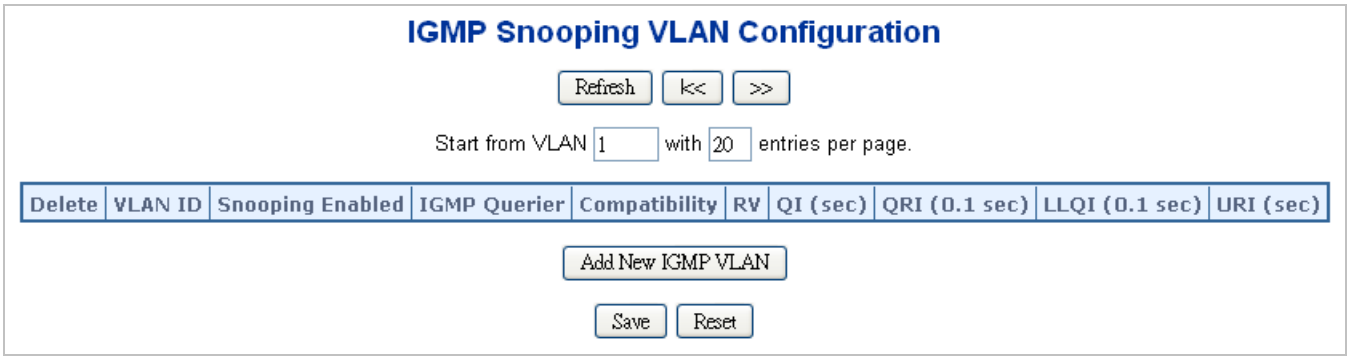


Figure 4-8-6: IGMP Snooping VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **IGMP Snooping Enable**	Enable the per-VLAN IGMP Snooping. Only up to 64 VLANs can be selected.

• **IGMP Querier**	Enable the IGMP Querier in the VLAN.
• **Compatibility**	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.
• **RV**	**Robustness Variable**. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.
• **QI**	**Query Interval**. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 255 seconds; default query interval is 125 seconds.
• **QRI**	**Query Response Interval**. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).
• **LLQI (LMQI for IGMP)**	**Last Member Query Interval**. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; default last member query interval is 10 in tenths of seconds (1 second).
• **URI**	**Unsolicited Report Interval**. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

<< : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

>> : Updates the table, starting with the entry after the last entry currently displayed.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.4 IGMP Snooping Port Group Filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service is based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace”. If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The IGMP Snooping Port Group Filtering Configuration screen in Figure 4-8-7 appears.

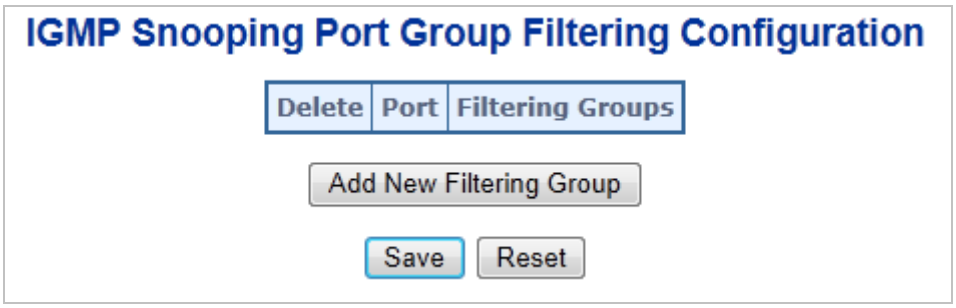


Figure 4-8-7: IGMP Snooping Port Group Filtering Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **Filtering Group**	The IP Multicast Group that will be filtered.

Buttons

Add New Filtering Group: Click to add a new entry to the Group Filtering table.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.5 IGMP Snooping Status

This page provides IGMP Snooping status. The IGMP Snooping Status screen in Figure 4-8-8 appears.

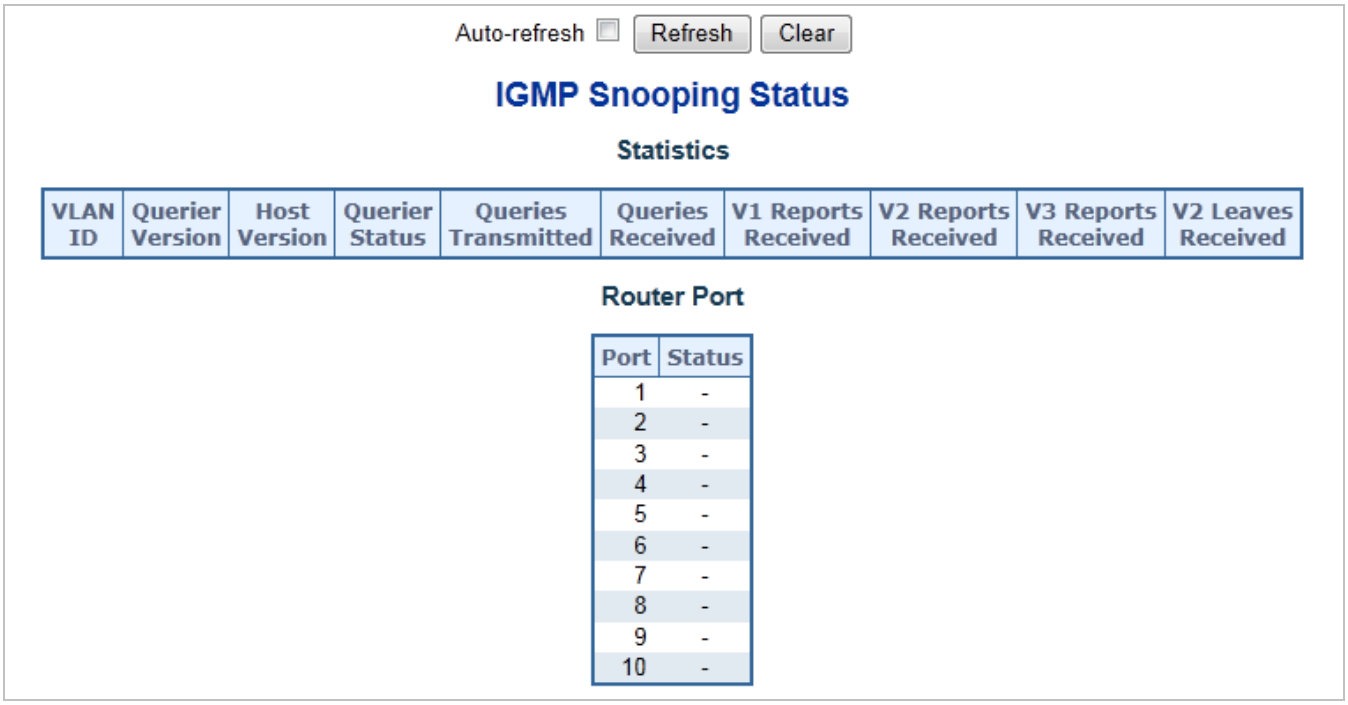


Figure 4-8-8: IGMP Snooping Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **Querier Version**	Working Querier Version currently.
• **Host Version**	Working Host Version currently.
• **Querier Status**	Show the Querier status is "ACTIVE" or "IDLE".
• **Queriers Transmitted**	The number of Transmitted Queriers.
• **Queriers Received**	The number of Received Queriers.
• **V1 Reports Received**	The number of Received V1 Reports.
• **V2 Reports Received**	The number of Received V2 Reports.
• **V3 Reports Received**	The number of Received V3 Reports.
• **V2 Leaves Received**	The number of Received V2 Leaves.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

4.8.6 IGMP Group Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field.

When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table.

The IGMP Groups Information screen in Figure 4-8-9 appears.

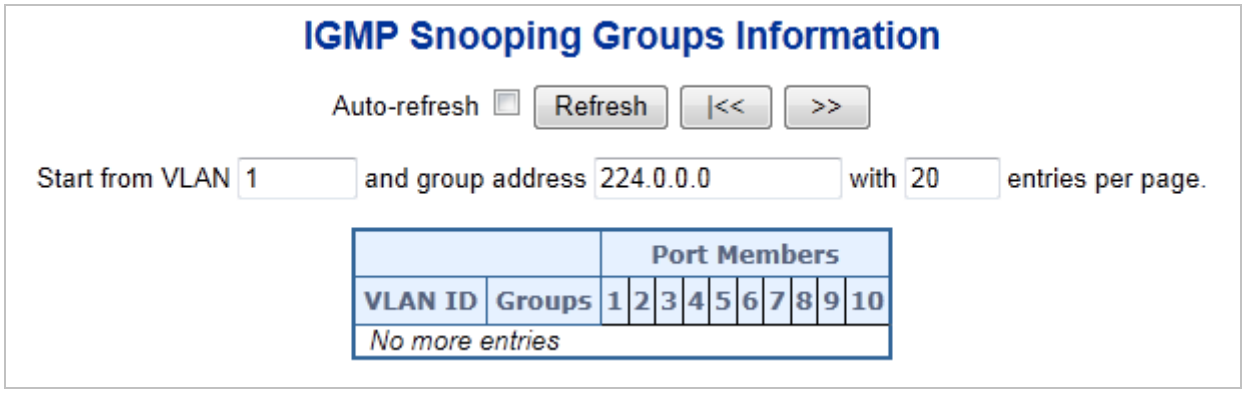


Figure 4-8-9: IGMP Snooping Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Groups**	Group address of the group displayed.
• **Port Members**	Ports under this group.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table, starting with the first entry in the IGMP Group Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.8.7 IGMPv3 Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "**Start from VLAN**", and "**Group**" input fields allow the user to select the starting point in the IGMP SFM Information Table.

The IGMPv3 Information screen in Figure 4-8-10 appears.

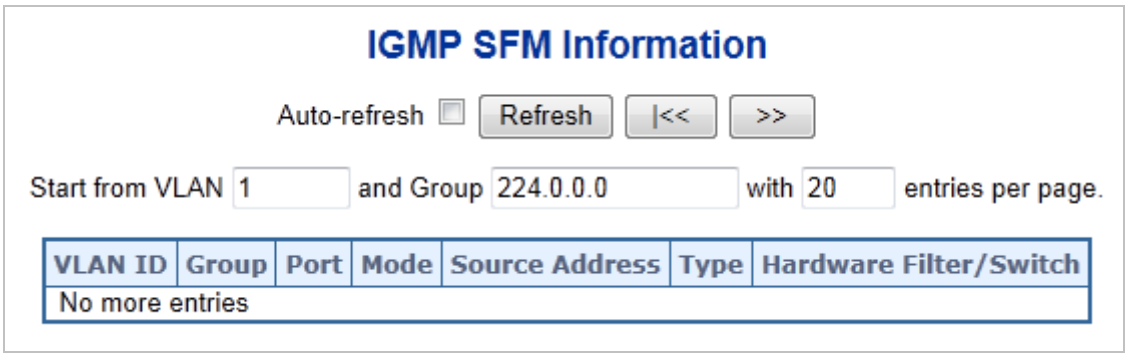


Figure 4-8-10: IGMP SFM Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Group**	Group address of the group displayed.
• **Port**	Switch port number.
• **Mode**	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• **Source Address**	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
• **Type**	Indicates the Type. It can be either Allow or Deny.
• **Hardware Filter / Switch**	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the table, starting with the first entry in the IGMP Group Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.8.8 MLD Snooping Configuration

This page provides MLD Snooping related configuration. The MLD Snooping Configuration screen in Figure 4-8-11 appears.

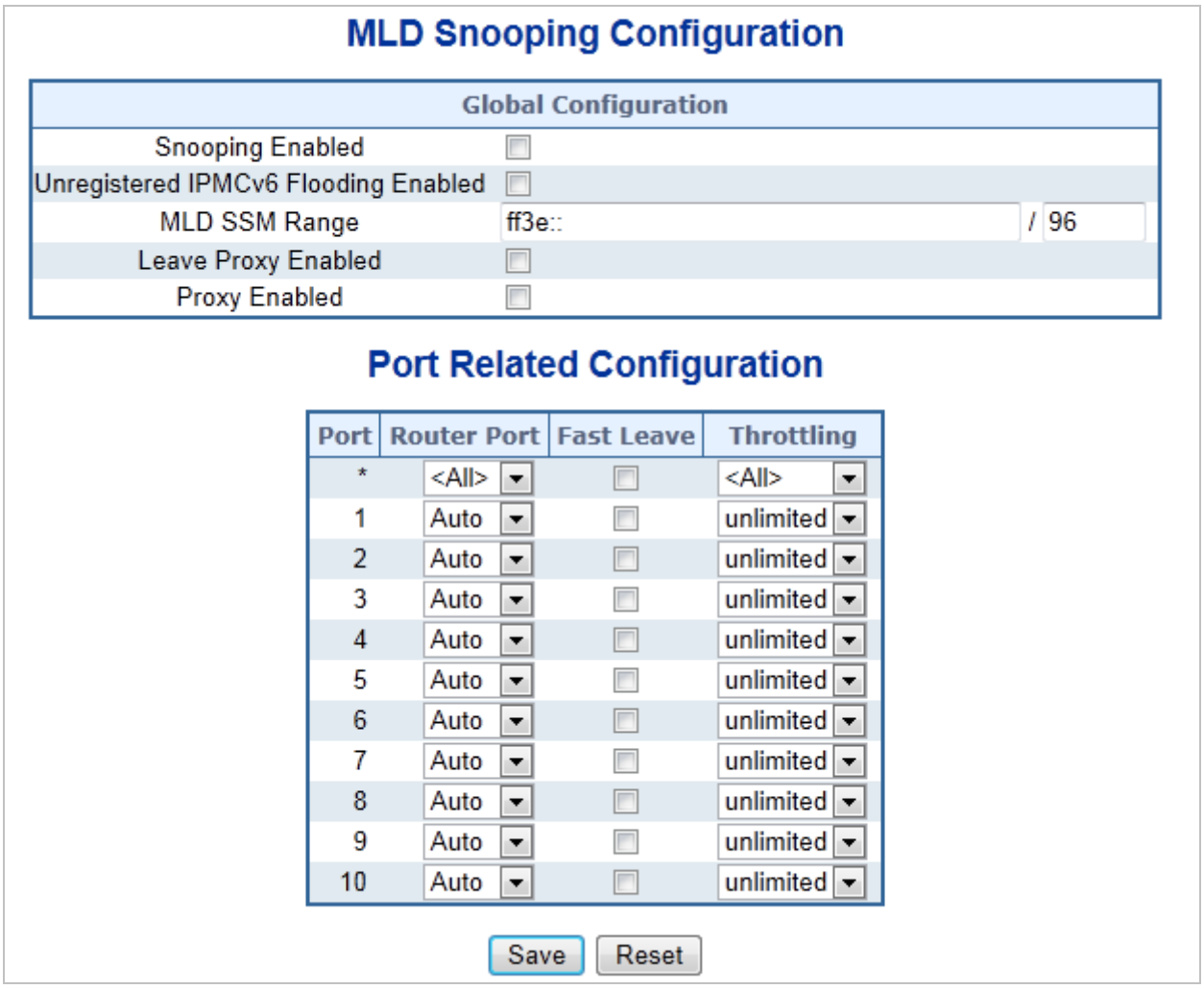


Figure 4-8-11: MLD Snooping Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Snooping Enabled**	Enable the Global MLD Snooping.
• **Unregistered IPMCv6 Flooding Enabled**	Enable unregistered IPMCv6 traffic flooding. Please note that disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.
• **MLD SSM Range**	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
• **Leave Proxy Enable**	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
• **Proxy Enable**	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
• **Router Port**	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. **All** means all ports will have one specific setting.
• **Fast Leave**	Enable the fast leave on the port.
• **Throttling**	The Configuration All with available values will assign to whole items. Enable to limit the number of multicast groups to which a switch port can belong. **All** means all ports will have one specific setting.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.9 MLD Snooping VLAN Configuration

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The MLD Snooping VLAN Configuration screen in Figure 4-8-12 appears.

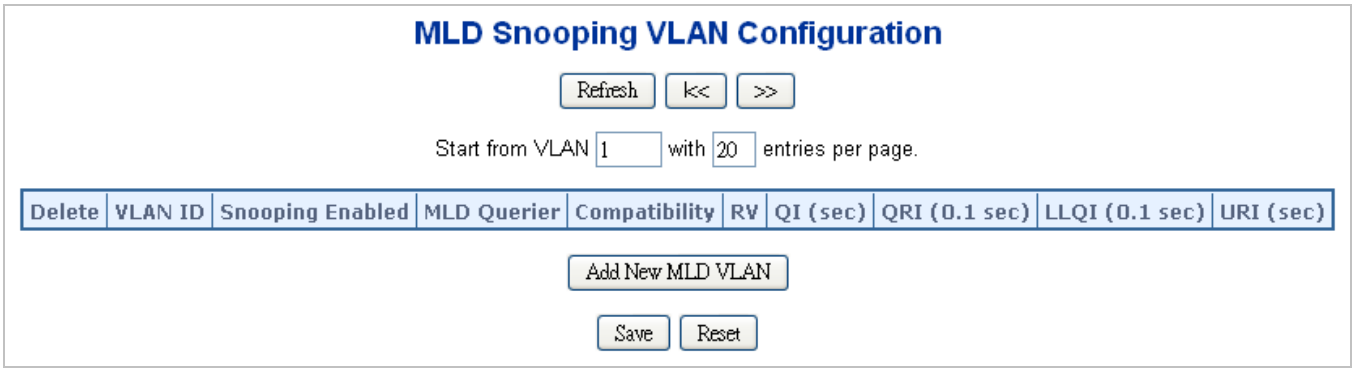


Figure 4-8-12: IGMP Snooping VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **MLD Snooping Enable**	Enable the per-VLAN MLD Snooping. Only up to 64 VLANs can be selected.
• **MLD Querier**	Enable the MLD Querier in the VLAN.
• **Compatibility**	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2; default compatibility value is MLD-Auto.
• **RV**	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is 1 to 255; default robustness variable value is 2.
• **QI**	Query Interval. The Query Interval variable denotes the interval between General Queries sent by the Querier. The allowed range is 1 to 255 seconds; default query interval is 125 seconds.
• **QRI**	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).
• **LLQI**	Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds; default last listener query interval is 10 in tenths of seconds (1 second).
• **URI**	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.10 MLD Snooping Port Group Filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service is based on a specific subscription plan. The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

MLD filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A MLD filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace”. If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group. The MLD Snooping Port Group Filtering Configuration screen in Figure 4-8-13 appears.

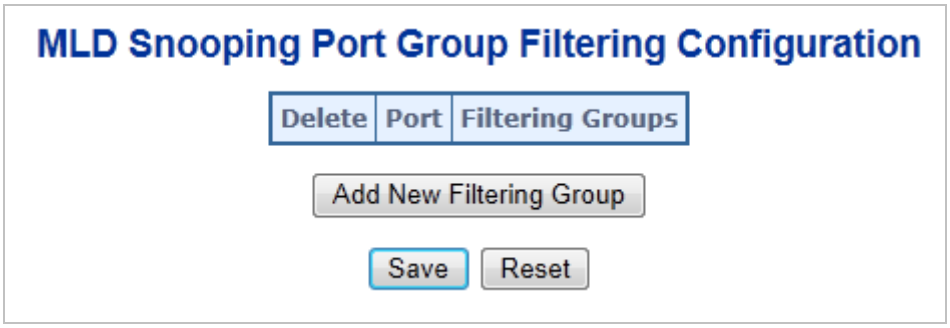


Figure 4-8-13: MLD Snooping Port Group Filtering Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **Filtering Group**	The IP Multicast Group that will be filtered.

Buttons

Add New Filtering Group: Click to add a new entry to the Group Filtering table.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.11 MLD Snooping Status

This page provides MLD Snooping status. The IGMP Snooping Status screen in Figure 4-8-14 appears.

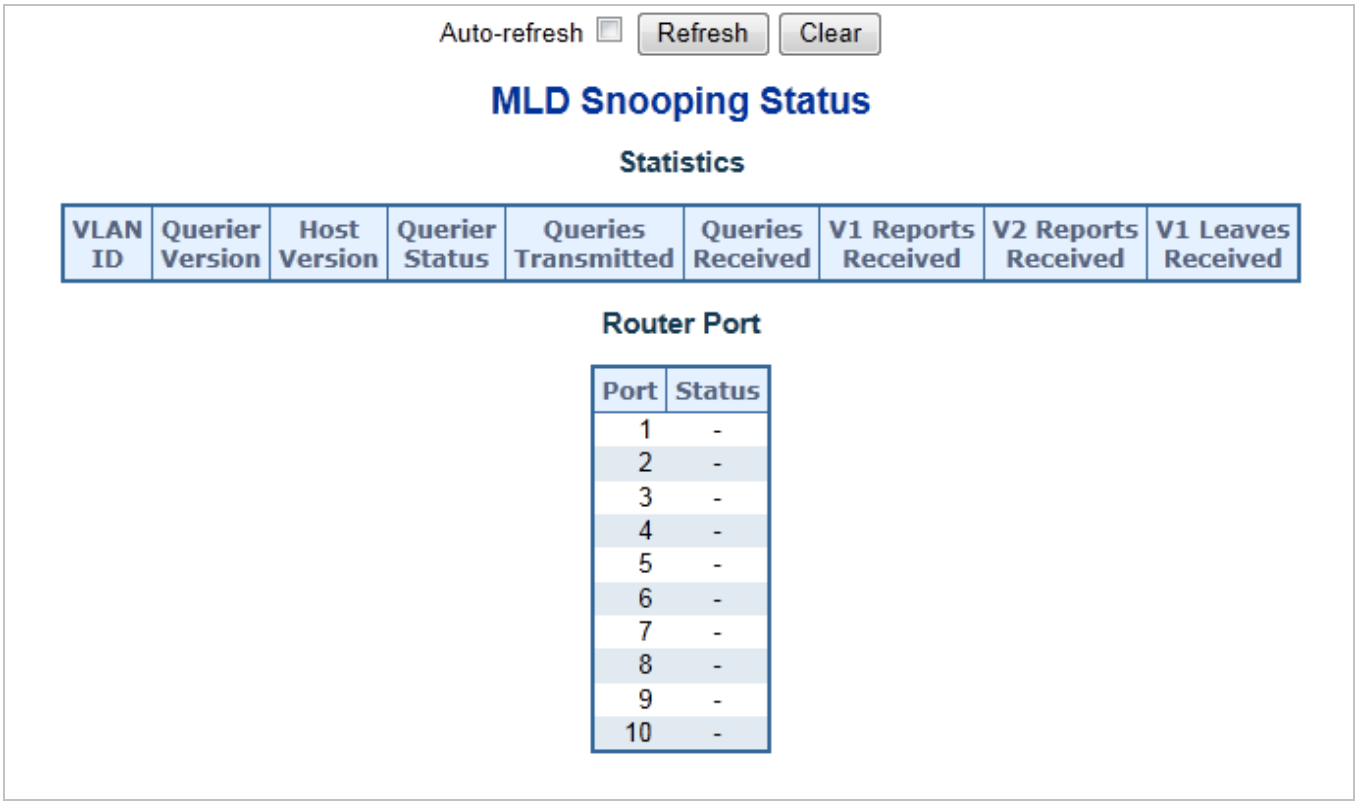


Figure 4-8-14: MLD Snooping Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The VLAN ID of the entry.
• **Querier Version**	Working Querier Version currently.
• **Host Version**	Working Host Version currently.
• **Querier Status**	Show the Querier status is "ACTIVE" or "IDLE".
• **Queriers Transmitted**	The number of Transmitted Queriers.
• **Queriers Received**	The number of Received Queriers
• **V1 Reports Received**	The number of Received V1 Reports
• **V2 Reports Received**	The number of Received V2 Reports
• **V1 Leave Received**	The number of Received V1 Leaves

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears MLD Snooping Status counters.

4.8.12 MLD Groups Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group. Each page shows up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table.

The MLD Groups Information screen in Figure 4-8-15 appears.

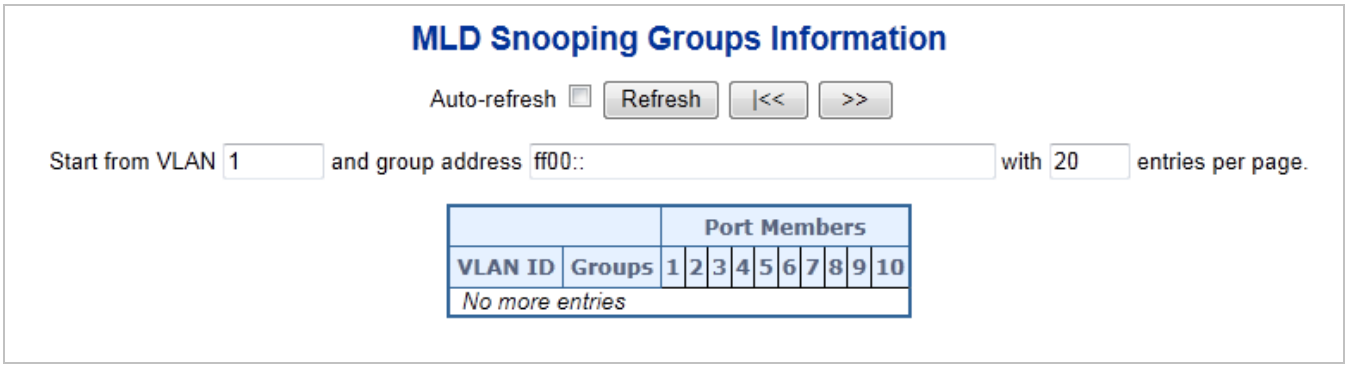


Figure 4-8-15: MLD Snooping Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Groups**	Group address of the group displayed.
• **Port Members**	Ports under this group.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table, starting with the first entry in the MLD Group Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.8.13 MLDv2 Information

Entries in the MLD SFM Information Table are shown on this page. The MLD **SFM (Source-Filtered Multicast)** Information Table also contains the **SSM (Source-Specific Multicast)** information. This table is sorted first by VLAN ID, then by group, and then by Port No. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 64 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SSM Information Table. The MLDv2 Information screen in Figure 4-8-16 appears.

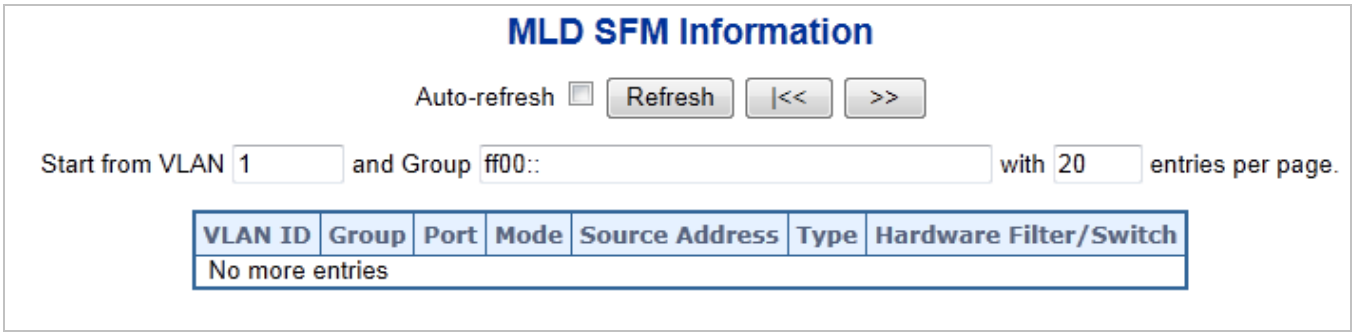


Figure 4-8-16: MLD SSM Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Group**	Group address of the group displayed.
• **Port**	Switch port number.
• **Mode**	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• **Source Address**	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
• **Type**	Indicates the Type. It can be either Allow or Deny.
• **Hardware Filter / Switch**	Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the MLD SFM Information.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.8.14 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLANs. In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports. It is allowed to create at maximum 8 MVR VLANs with corresponding channel settings for each Multicast VLAN. There will be totally at maximum 256 group addresses for channel settings.

This page provides MVR related configuration. The MVR screen in Figure 4-8-17 appears.

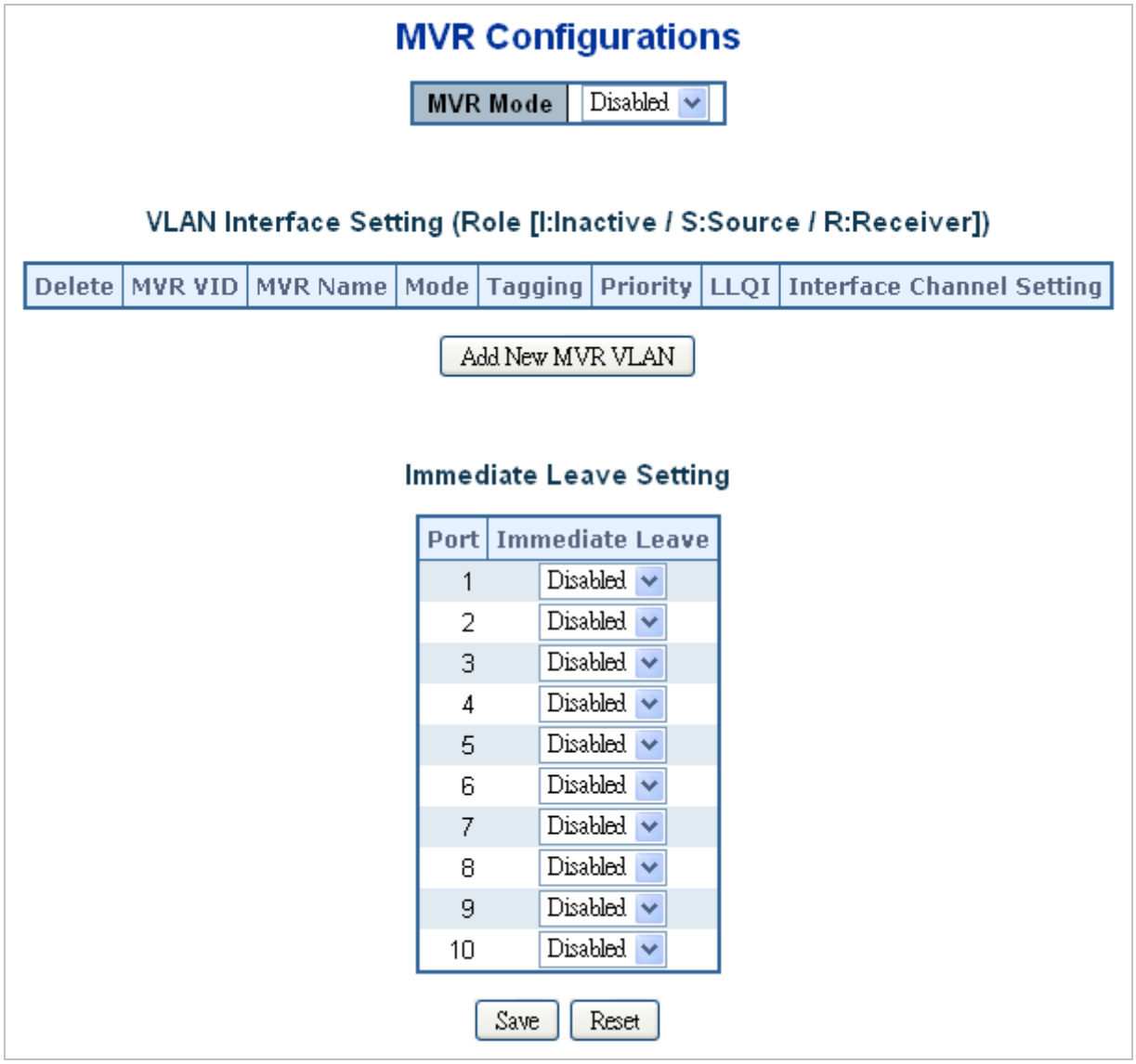


Figure 4-8-17: MVR Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **MVR Mode**	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.
• **Delete**	Check to delete the entry. The designated entry will be deleted during the next save.
• **MVR VID**	Specify the Multicast VLAN ID. **Be Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports.
• **MVR Name**	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
• **Mode**	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
• **Tagging**	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
• **Priority**	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
• **LLQI**	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
• **Interface Channel Setting**	When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.
• **Port**	The logical port for the settings.
• **Port Role**	Configure an MVR port of the designated MVR VLAN as one of the following roles. ■ **Inactive**: The designated port does not participate in MVR operations. **Source**: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. ■ **Receiver**: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. ■ **Be Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicate Inactive; S indicates Source; R indicates Receiver The default Role is Inactive.
• **Immediate Leave**	Enable the fast leave on the port.

Buttons

Add New MVR VLAN: Click to add new MVR VLAN. Specify the VID and configure the new entry. Click "Save"

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.8.15 MVR Status

This page provides MVR status. The MVR Status screen in Figure 4-8-18 appears.

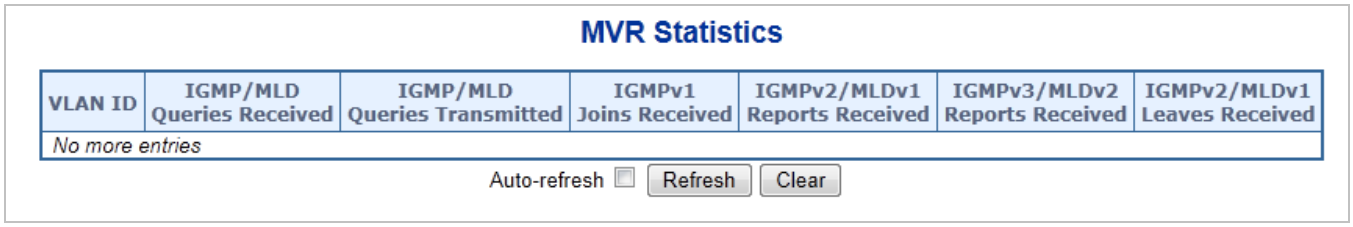


Figure 4-8-18: MVR Status Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	The Multicast VLAN ID
• **IGMP/MLD Queries Received**	The number of Received Queries for IGMP and MLD, respectively.
• **IGMP/MLD Queries Transmitted**	The number of Transmitted Queries for IGMP and MLD, respectively.
• **IGMPv1 Joins Received**	The number of Received IGMPv1 Joins.
• **IGMPv2/MLDv1 Reports Received**	The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.
• **IGMPv3/MLDv2 Reports Received**	The number of Received IGMPv3 Joins and MLDv2 Reports, respectively.
• **IGMPv2/MLDv1 Leaves Received**	The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears MVR Statistics counters.

4.8.16 MVR Groups Information

Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field.

When first visited, the web page will show the first 20 entries from the beginning of the MVR Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MVR Group Table.

The MVR Groups Information screen in Figure 4-8-19 appears.

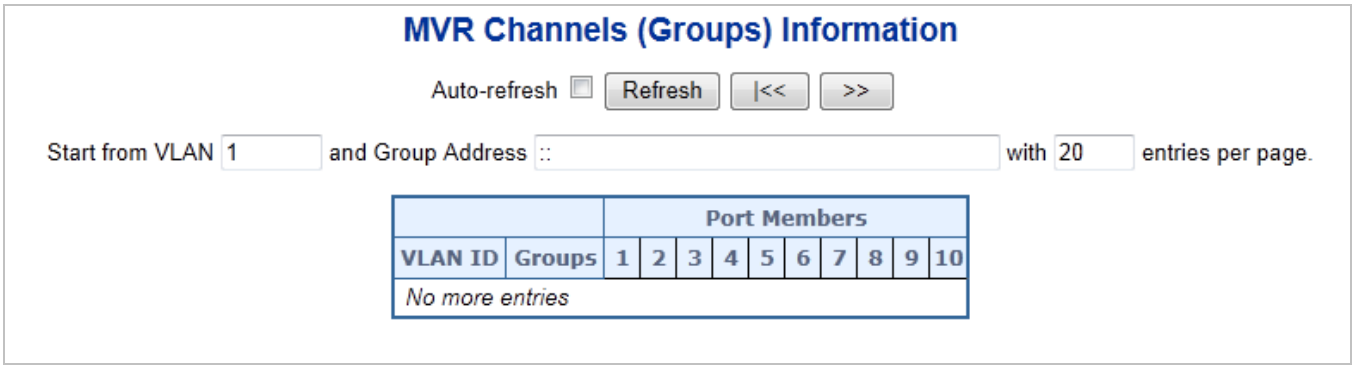


Figure 4-8-19: MVR Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Groups**	Group ID of the group displayed.
• **Port Members**	Ports under this group.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.8.17 MVR SFM Information

Entries in the MVR SFM Information Table are shown on this page. The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

The MVR Groups Information screen in Figure 4-8-20 appears.

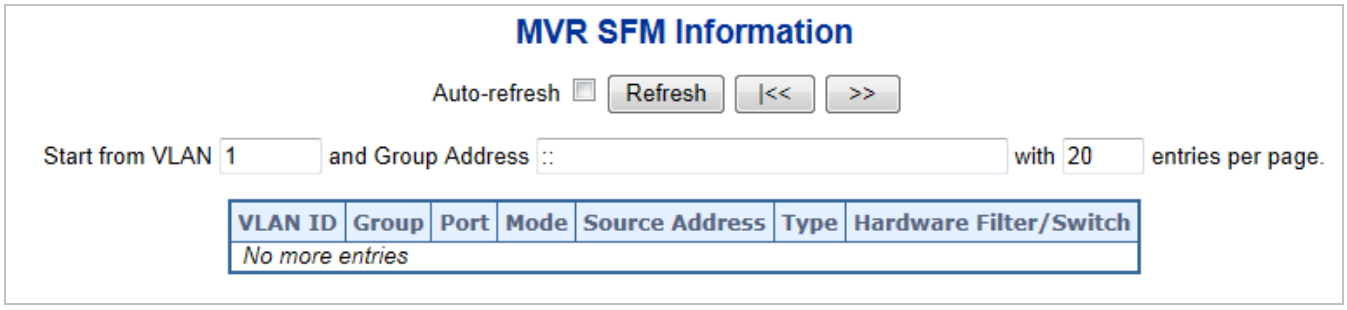


Figure 4-8-20: MVR Groups Information Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN ID**	VLAN ID of the group.
• **Group**	Group ID of the group displayed.
• **Port**	Switch port number.
• **Mode**	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
• **Source Address**	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.
• **Type**	Indicates the Type. It can be either Allow or Deny.
• **Hardware Filter / Switch**	Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the table starting from the first entry in the MVR SFM Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.9 Quality of Service

4.9.1 Understand QOS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic. You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

QoS Terminology

- **Classifier**—classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The Switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** — is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level**—defines the priority that will be given to a set of classified traffic. You can create and modify service levels.
- **Policy**—comprises a set of “rules” that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile**—consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules**—comprises a service level and a classifier to define how the Switch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

To implement QoS on your network, you need to carry out the following actions:

1. Define a service level to determine the priority that will be applied to traffic.

2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.

3. Create a QoS profile which associates a service level and a classifier.

4. Apply a QoS profile to a port(s).

4.9.2 Port Policing

This page allows you to configure the Policer settings for all switch ports. The Port Policing screen in Figure 4-9-1 appears.

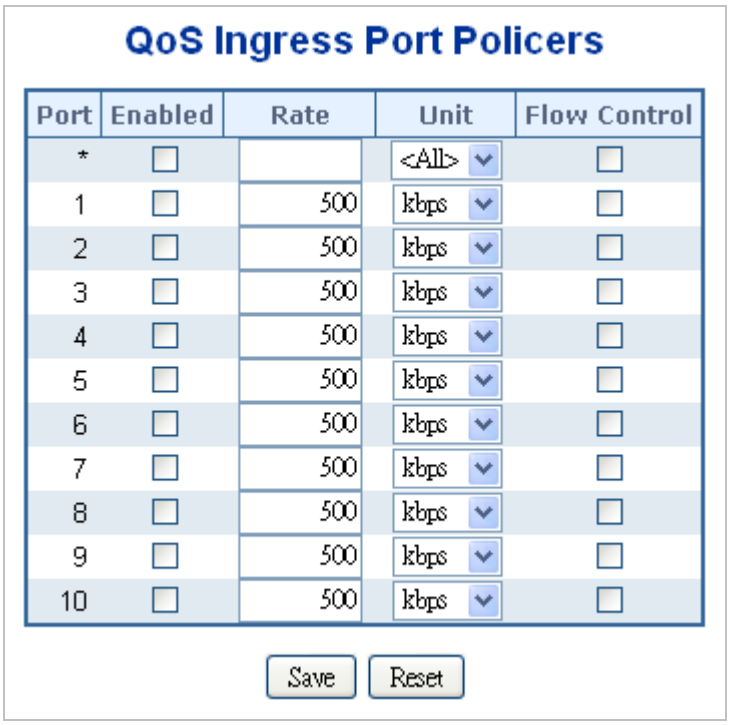


Figure 4-9-1: QoS Ingress Port Policers Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Enabled**	Controls whether the policer is enabled on this switch port, * means selection all ports of Industrial Managed Switch.
• **Rate**	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the **"Unit**" is **"kbps"** or **"fps"**, and it is restricted to 1-3300 when the **"Unit"** is **"Mbps"** or **"kfps"**.
• **Unit**	The Configuration All with available options will assign to whole ports. Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps. The default value is **"kbps"**. **All** means all ports will have one specific setting.
• **Flow Control**	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

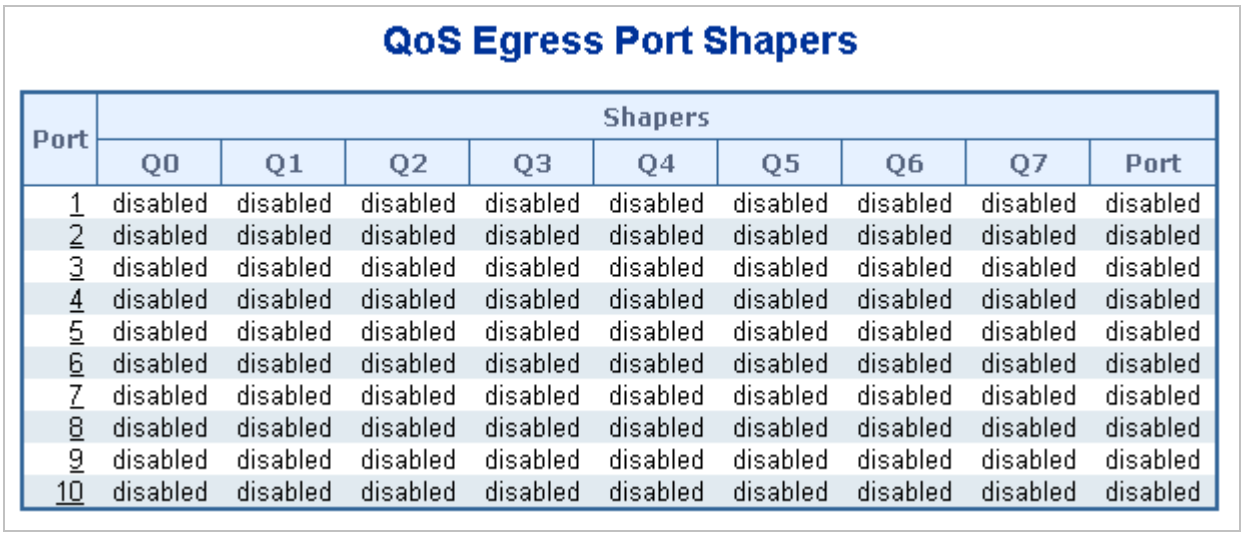
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.9.3 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports. The Port Shaping screen in Figure 4-9-2 appears.



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Figure 4-9-2: QoS Egress Port Shapers Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers. For more detail, please refer to chapter 4.9.3.1.
• **Q0 ~Q7**	Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".
• **Port**	Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

4.9.3.1 QoS Egress Port Schedule and Shapers

The Port Scheduler and Shapers for a specific port are configured on this page. The QoS Egress Port Schedule and Shaper screen in Figure 4-9-3 appears.

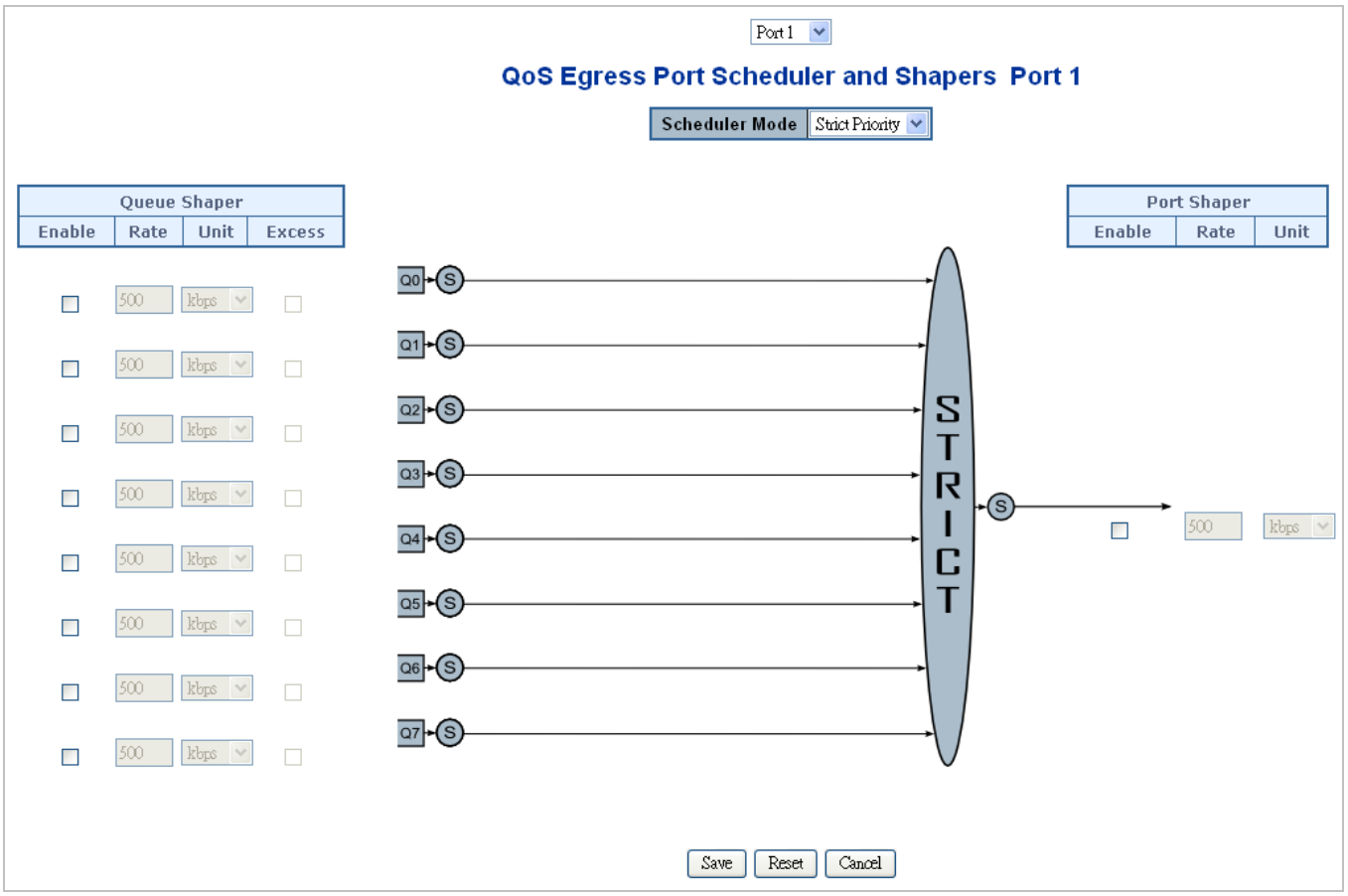


Figure 4-9-3: QoS Egress Port Schedule and Shapers Page Screenshot

The page includes the following fields:

Object	Description
• **Schedule Mode**	Controls whether the scheduler mode is **"Strict Priority"** or **"Weighted"** on this switch port.
• **Queue Shaper Enable**	Controls whether the queue shaper is enabled for this queue on this switch port.
• **Queue Shaper Rate**	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the **"Unit"** is **"kbps"**, and it is restricted to 1-3300 when the "Unit" is "Mbps".
• **Queue Shaper Unit**	Controls the unit of measure for the queue shaper rate as **"kbps"** or **"Mbps"**. The default value is **"kbps"**.
• **Queue Shaper Excess**	Controls whether the queue is allowed to use excess bandwidth.
• **Queue Scheduler Weight**	Controls the weight for this queue. The default value is **"17"**. This value is restricted to 1-100. This parameter is only shown if **"Scheduler Mode"** is set to **"Weighted"**.
• **Queue Scheduler Percent**	Shows the weight in percent for this queue. This parameter is only shown if **"Scheduler Mode"** is set to **"Weighted".**
• **Port Shaper Enable**	Controls whether the port shaper is enabled for this switch port.
• **Port Shaper Rate**	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the **"Unit"** is **"kbps"**, and it is restricted to 1-3300 when the **"Unit"** is **"Mbps"**.
• **Port Shaper Unit**	Controls the unit of measure for the port shaper rate as **"kbps"** or **"Mbps"**. The default value is **"kbps"**.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the previous page.

4.9.4 Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports. The Port Classification screen in Figure 4-9-4 appears.

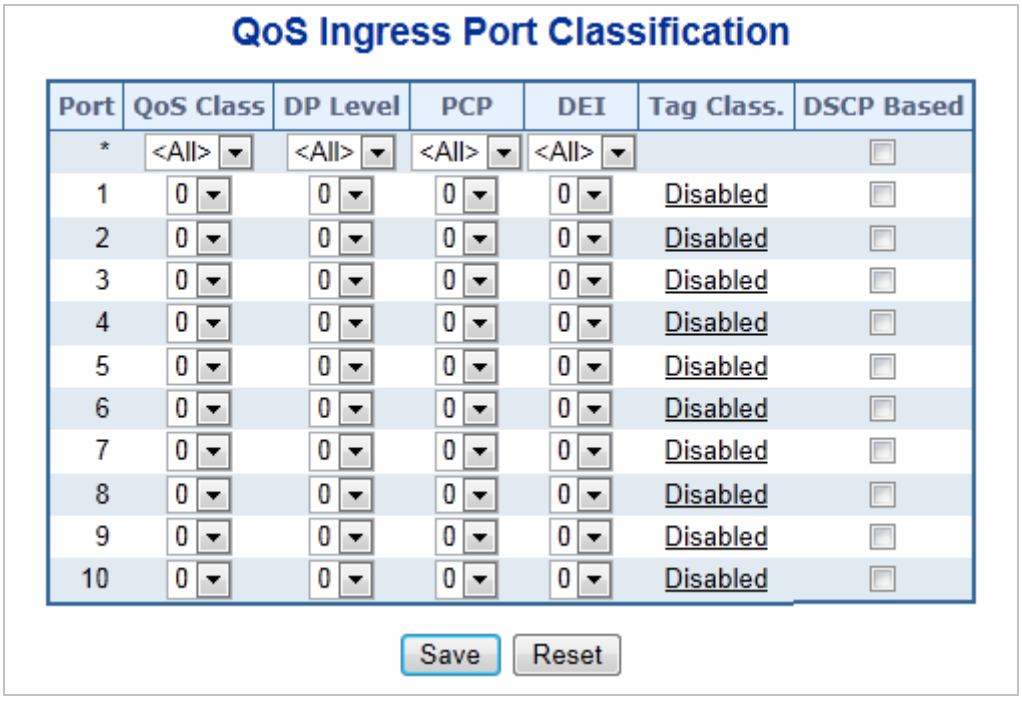


Figure 4-9-4 : QoS Ingres Port Classification Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **QoS Class**	The Configuration All with available values will assign to whole ports. Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority. **All** means all ports will have one specific setting.
• **DP Level**	The Configuration All with available values will assign to whole ports. Controls the default DP level, i.e., the DP level for frames not classified in any other way. **All** means all ports will have one specific setting.
• **PCP**	The Configuration All with available values will assign to whole ports. Controls the default PCP for untagged frames. **All** means all ports will have one specific setting.
• **DEI**	The Configuration All with available values will assign to whole ports. Controls the default DEI for untagged frames. **All** means all ports will have one specific setting.

• **Tag Class**	Shows the classification mode for tagged frames on this port. ■ **Disabled**: Use default QoS class and DP level for tagged frames. ■ **Enabled**: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. For more detail information, please refer to chapter 4.9.3.1.
• **DSCP Based**	Click to Enable DSCP Based QoS Ingress Port Classification.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.9.4.1 QoS Ingress Port Tag Classification

The classification modes for tagged frames are configured on this page. The QoS Ingress Port Tag Classification screen in Figure 4-9-5 appears.

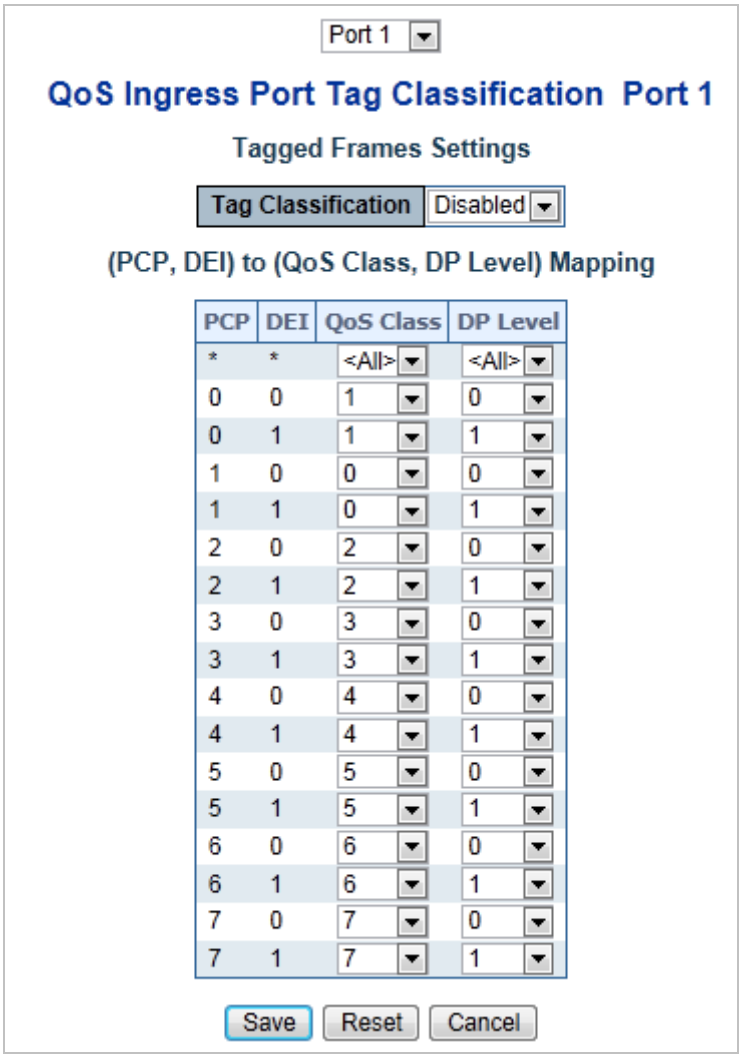


Figure 4-9-5 : QoS Ingres Port Tag Classification Page Screenshot

The page includes the following fields:

Object	Description
• **Tag Classification**	Controls the classification mode for tagged frames on this port. ■ **Disabled**: Use default QoS class and DP level for tagged frames. ■ **Enabled**: Use mapped versions of PCP and DEI for tagged frames.
• **(PCP, DEI) to (QoS class, DP level) Mapping**	The Configuration All with available values will assign to whole items. Controls the mapping of the classified (PCP, DEI) to (QoS class, DP level) values when Tag Classification is set to **Enabled**.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Return to the previous page.

4.9.5 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports. The Port Scheduler screen in Figure 4-9-6 appears.

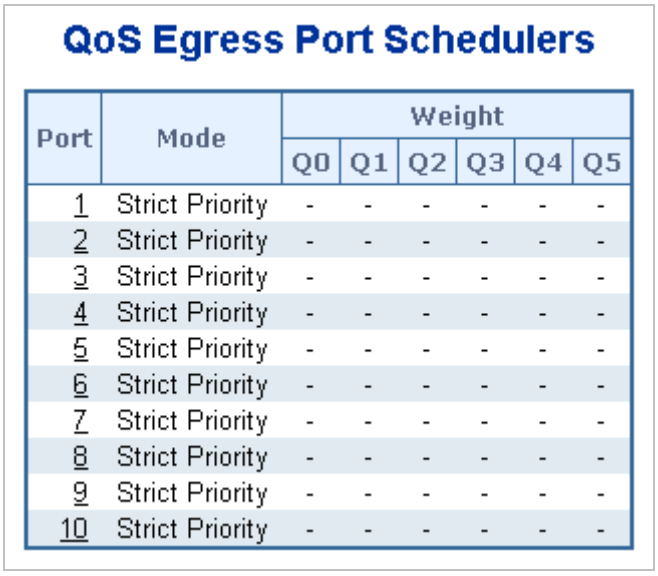

QoS Egress Port Schedulers
Port
Mode
Weight
Q0 Q1 Q2 Q3 Q4 Q5
1 Strict Priority - - - - - -
2 Strict Priority - - - - - -
3 Strict Priority - - - - - -
4 Strict Priority - - - - - -
5 Strict Priority - - - - - -
6 Strict Priority - - - - - -
7 Strict Priority - - - - - -
8 Strict Priority - - - - - -
9 Strict Priority - - - - - -
10 Strict Priority - - - - - -

Figure 4-9-6: QoS Egress Port Schedule Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers. For more detail, please refer to chapter 4.9.5.1.
• **Mode**	Shows the scheduling mode for this port.
• **Q0 ~ Q5**	Shows the weight for this queue and port.

4.9.6 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports. The Port Tag Remarking screen in Figure 4-9-7 appears.

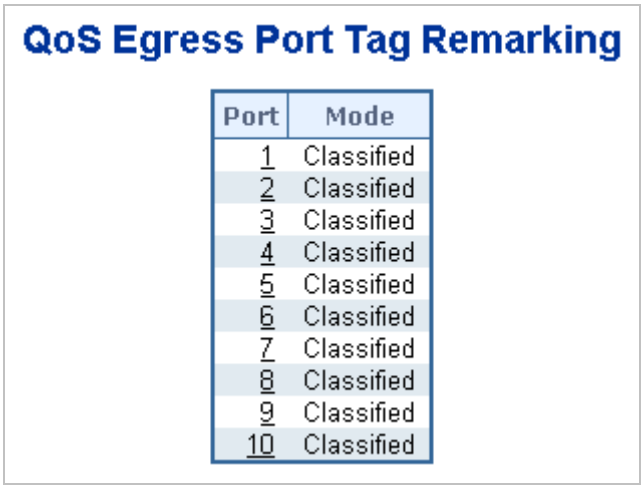


Figure 4-9-7: QoS Egress Port Tag Remarking Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking. For more detail, please refer to chapter 4.9.6.1.
• **Mode**	Shows the tag remarking mode for this port. ■ **Classified**: Use classified PCP/DEI values. ■ **Default**: Use default PCP/DEI values. ■ **Mapped**: Use mapped versions of QoS class and DP level.

4.9.6.1 QoS Egress Port Tag Remarking

The QoS Egress Port Tag Remarking for a specific port is configured on this page. The QoS Egress Port Tag Remarking screen in Figure 4-9-8 appears.

Figure 4-9-8: QoS Egress Port Tag Remarking Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Controls the tag remarking mode for this port. ■ **Classified**: Use classified PCP/DEI values. ■ **Default**: Use default PCP/DEI values. ■ **Mapped**: Use mapped versions of QoS class and DP level.
• **PCP/DEI Configuration**	Controls the default PCP and DEI values used when the mode is set to **Default**.
• **(QoS class, DP level) to (PCP, DEI) Mapping**	Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to **Mapped**.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the previous page.

4.9.7 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports. The Port DSCP screen in Figure 4-9-9 appears.

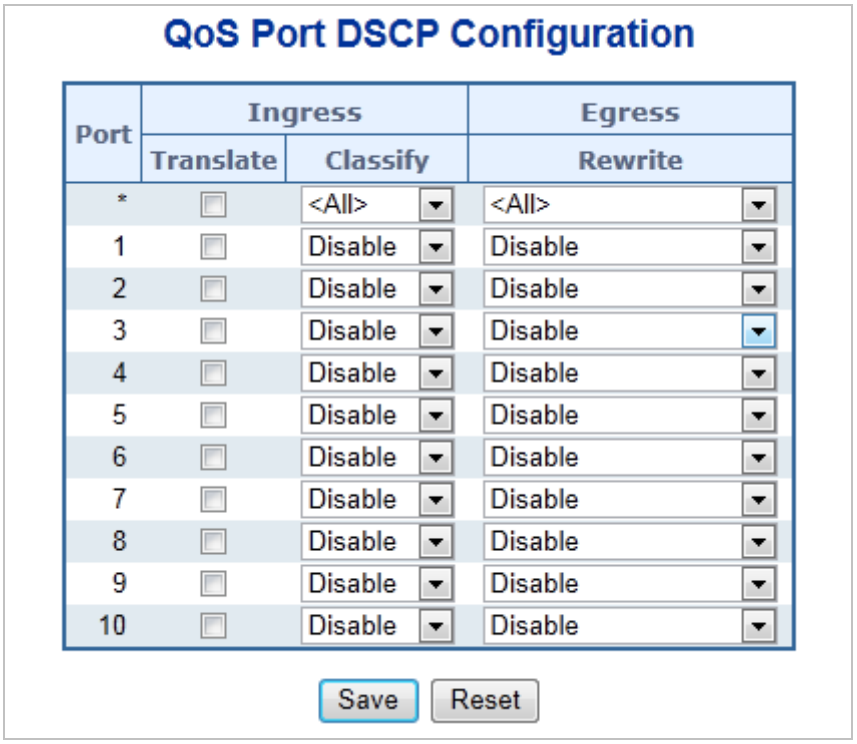


Figure 4-9-9 : QoS Port DSCP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
• **Ingress**	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: ■ **Translate** ■ **Classify**
• **Translate**	To Enable the Ingress Translation click the checkbox. * means to select all ports of Industrial Managed Switch.
• **Classify**	The Configuration All with available options will assign to whole ports. Classification for a port has 4 different values. All means all ports will have one specific setting. ■ **Disable**: No Ingress DSCP Classification. ■ **DSCP=0**: Classify if incoming (or translated if enabled) DSCP is 0. ■ **Selected**: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. ■ **All**: Classify all DSCP.
• **Egress**	The Configuration All with available options will assign to whole ports. Port Egress Rewriting can be one of –. All means all ports will have one specific setting. ■ **Disable**: No Egress rewrite. ■ **Enable**: Rewrite enabled without remapping. ■ **Remap DP Unaware**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. ■ **Remap DP Aware**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.9.8 DSCP-Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches. The DSCP-Based QoS screen in Figure 4-9-10 appears.

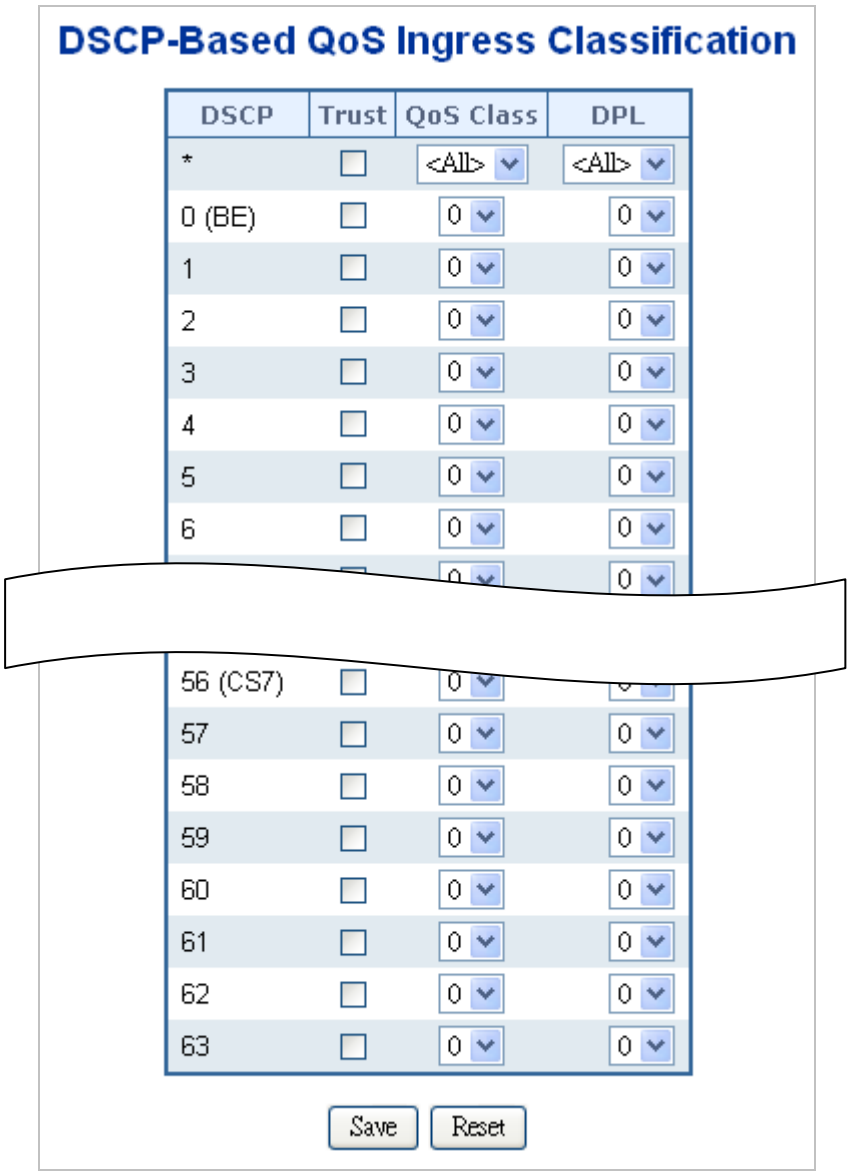


Figure 4-9-10: DSCP-Based QoS Ingress Classification Page Screenshot

The page includes the following fields:

Object	Description
• **DSCP**	Maximum number of supported DSCP values is 63.
• **Trust**	Click to check if the DSCP value is trusted. * means to select all ports of Industrial Managed Switch.
• **QoS Class**	The Configuration All with available values will assign to whole DSCP values. QoS Class value can be any of (0-7)
• **DPL**	The Configuration All with available values will assign to whole DSCP values. Drop Precedence Level (0-1)

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.9.9 DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress. The DSCP Translation screen in Figure 4-9-11 appears.

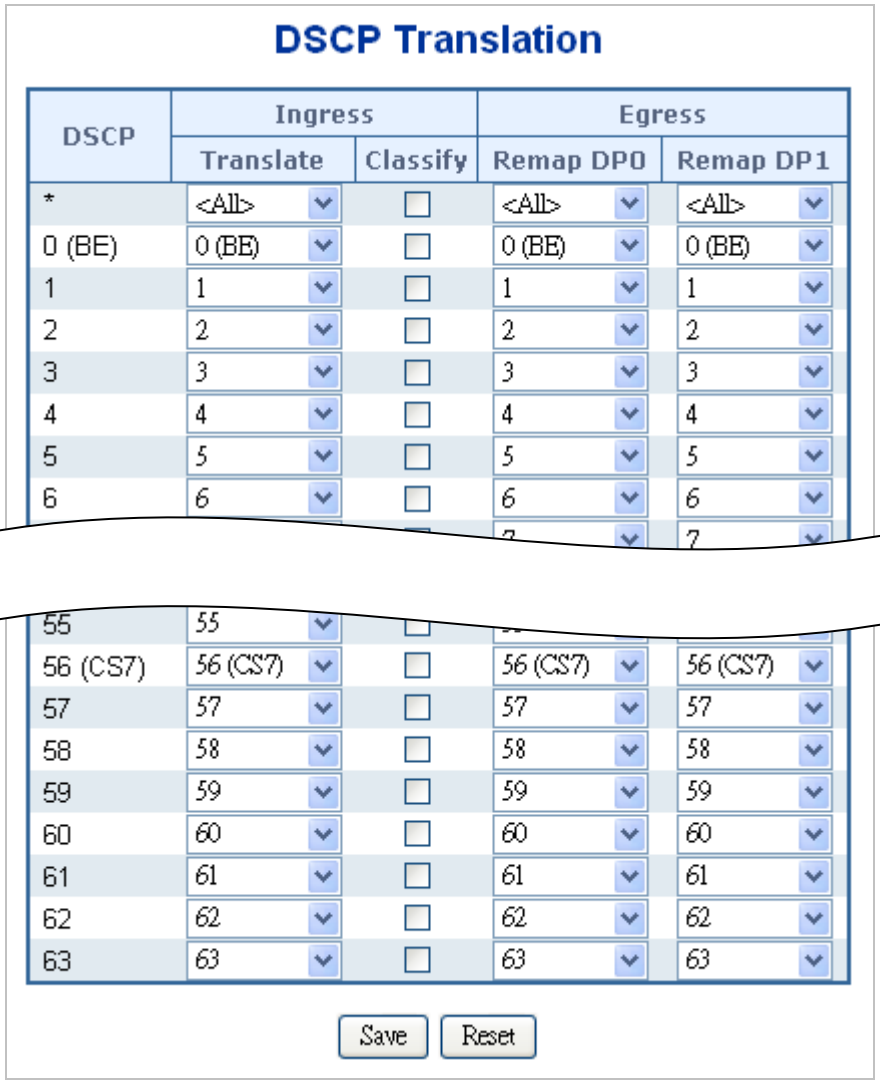


Figure 4-9-11: DSCP Translation Page Screenshot

The page includes the following fields:

Object	Description
• **DSCP**	Maximum numbers of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
• **Ingress**	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation – ■ **Translate** ■ **Classify**
• **Translate**	The Configuration All with available values will assign to whole DSCP values. DSCP at Ingress side can be translated to any of (0-63) DSCP values.
• **Classify**	Click to enable Classification at Ingress side.
• **Egress**	There are the following configurable parameters for Egress side – ■ **Remap DP0** Controls the remapping for frames with DP level 0. ■ **Remap DP1** Controls the remapping for frames with DP level 1.
• **Remap DP0**	The Configuration All with available values will assign to whole DSCP values. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.
• **Remap DP1**	The Configuration All with available values will assign to whole DSCP values. Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.9.10 DSCP Classification

This page allows you to map DSCP value to a QoS Class and DPL value. The DSCP Classification screen in Figure 4-9-12 appears.

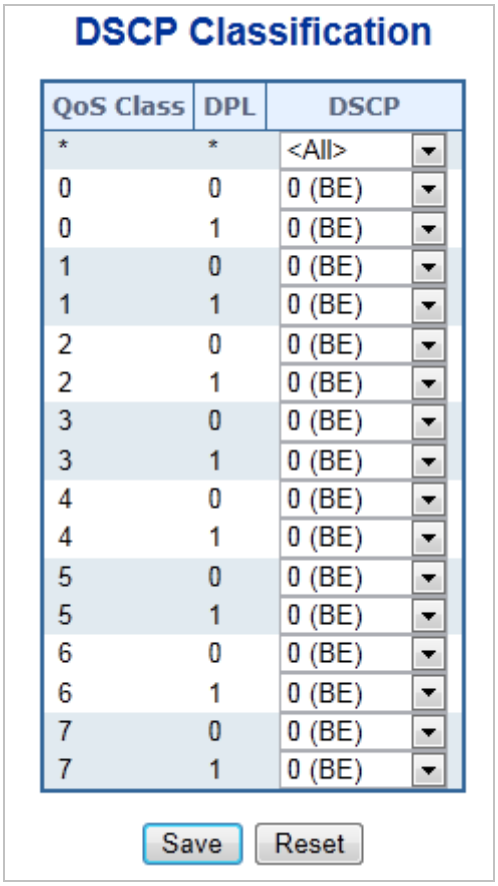


Figure 4-9-12: DSCP Classification Page Screenshot

The page includes the following fields:

Object	Description
• **QoS Class**	Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.
• **DPL**	Drop Precedence Level (0-1) can be configured for all available QoS Classes.
• **DSCP**	The Configuration All with available values will assign to whole QoS Class. Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.9.11 QoS Control List

This page shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch.

Click on the lowest plus sign to add a new QCE to the list.

The QoS Control List screen in Figure 4-9-13 appears.

Figure 4-9-13: QoS Control List Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **QCE#**	Indicates the index of QCE.
• **Port**	Indicates the list of ports configured with the QCE.
• **Frame Type**	Indicates the type of frame to look for incoming frames. Possible frame types are: ■ **Any**: The QCE will match all frame type. ■ **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. ■ **LLC**: Only (LLC) frames are allowed. ■ **SNAP**: Only (SNAP) frames are allowed. ■ **IPv4**: The QCE will match only IPV4 frames. ■ **IPv6**: The QCE will match only IPV6 frames.
• **SMAC**	Displays the OUI field of Source MAC address, i.e. first three octet (byte) of MAC address.
• **DMAC**	Specify the type of Destination MAC addresses for incoming frame. Possible values are: ■ **Any**: All types of Destination MAC addresses are allowed. ■ **Unicast**: Only Unicast MAC addresses are allowed. ■ **Multicast**: Only Multicast MAC addresses are allowed. ■ **Broadcast**: Only Broadcast MAC addresses are allowed. The default value is 'Any'.
• **VID**	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
• **PCP**	Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
• **DEI**	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.
• **Action**	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. ■ **Class**: Classified QoS Class; if a frame matches the QCE it will be put in the queue. ■ **DPL**: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. ■ **DSCP**: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
• **Modification Buttons**	You can modify each QCE in the table using the following buttons: ⊕: Inserts a new QCE before the current row. ⓔ: Edits the QCE.

	: Moves the QCE up the list. : Moves the QCE down the list. : Deletes the QCE. : The lowest plus sign adds a new entry at the bottom of the list of QCL.

4.9.11.1 QoS Control Entry Configuration

The QCE Configuration screen in Figure 4-9-14 appears.

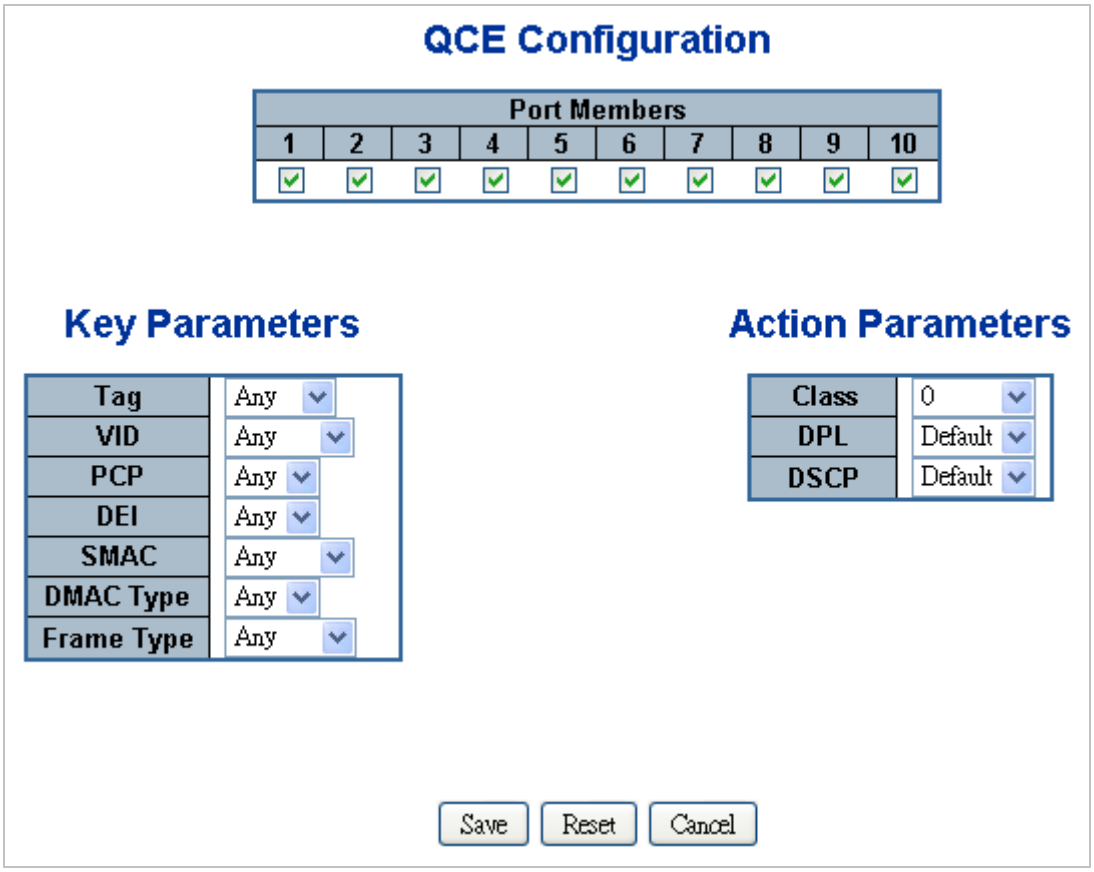


Figure 4-9-14: QCE Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Members**	Check the checkbox button in case you what to make any port member of the QCL entry. By default all ports will be checked
• **Key Parameters**	Key configuration is described as below: ■ **Tag** Value of Tag field can be 'Any', 'Untag' or 'Tag'. ■ **VID** Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs. ■ **PCP** Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. ■ **DEI** Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'. ■ **SMAC** Source MAC address: 24 MS bits (OUI) or 'Any'. ■ **DMAC Type** Destination MAC type: possible values are unicast (UC), multicast (MC), broadcast (BC) or 'Any'. ■ **Frame Type** Frame Type can have any of the following values: 1. **Any** 2. **Ethernet** 3. **LLC** 4. **SNAP**

	5. **IPv4** 6. **IPv6** Note: All frame types are explained below.
• **Any**	Allow all types of frames.
• **Ethernet**	**Ethernet Type** Valid Ethernet type can have value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD (IPv6), default value is 'Any'.
• **LLC**	■ **SSAP Address** Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' ■ **DSAP Address** Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' ■ **Control Address** Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'
• **SNAP**	**PID** Valid PID(a.k.a Ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'
• **IPv4**	■ **Protocol** IP protocol number: (0-255, TCP or UDP) or 'Any' ■ **Source IP** Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero **DSCP** Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43 ■ **IP Fragment** IPv4 frame fragmented option: yes|no|any ■ **Sport** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP ■ **Dport** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
• **IPv6**	■ **Protocol** IP protocol number: (0-255, TCP or UDP) or 'Any' ■ **Source IP** IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits ■ **DSCP** Diffserv Code Point value (DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43 ■ **Sport** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP ■ **Dport** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
• **Action Parameters**	■ **Class** QoS class: (0-7) or 'Default'. ■ **DP** Valid Drop Precedence Level can be (0-1) or 'Default'. ■ **DSCP** Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'. 'Default' means that the default classified value is not modified by this QCE.

Buttons

Save: Click to save the configuration and move to main QCL page

Reset: Click to undo any changes made locally and revert to previously saved values

Cancel: Return to the previous page without saving the configuration change

4.9.12 QoS Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is **256** on each switch. The QoS Control List Status screen in Figure 4-9-15 appears.

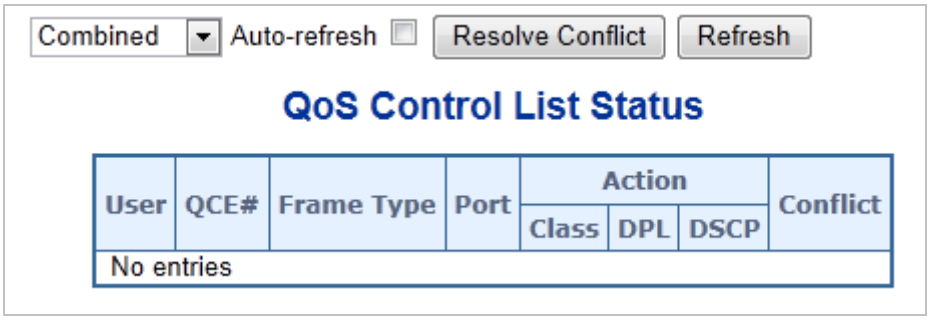


Figure 4-9-15: QoS Control List Status Page Screenshot

The page includes the following fields:

Object	Description
• **User**	Indicates the QCL user.
• **QCE#**	Indicates the index of QCE.
• **Frame Type**	Indicates the type of frame to look for incoming frames. Possible frame types are: ■ **Any**: The QCE will match all frame type. ■ **Ethernet**: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. ■ **LLC**: Only (LLC) frames are allowed. ■ **SNAP**: Only (SNAP) frames are allowed. ■ **IPv4**: The QCE will match only IPV4 frames. ■ **IPv6**: The QCE will match only IPV6 frames.
• **Port**	Indicates the list of ports configured with the QCE
• **Action**	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. ■ **Class**: Classified QoS Class; if a frame matches the QCE it will be put in the queue. ■ **DPL**: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. ■ **DSCP**: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
• **Conflict**	Displays QCE status. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the resource required by the QCE and pressing 'Refresh' button.

Buttons

Combined: Select the QCL status from this drop down list.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Resolve Conflict: Click to release the resources required to add QCL entry, incase conflict status for any QCL entry is 'yes'.

Refresh: Click to refresh the page immediately.

4.9.13 Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports. The QoS Ingress Queue Policers screen in Figure 4-9-16 appears.

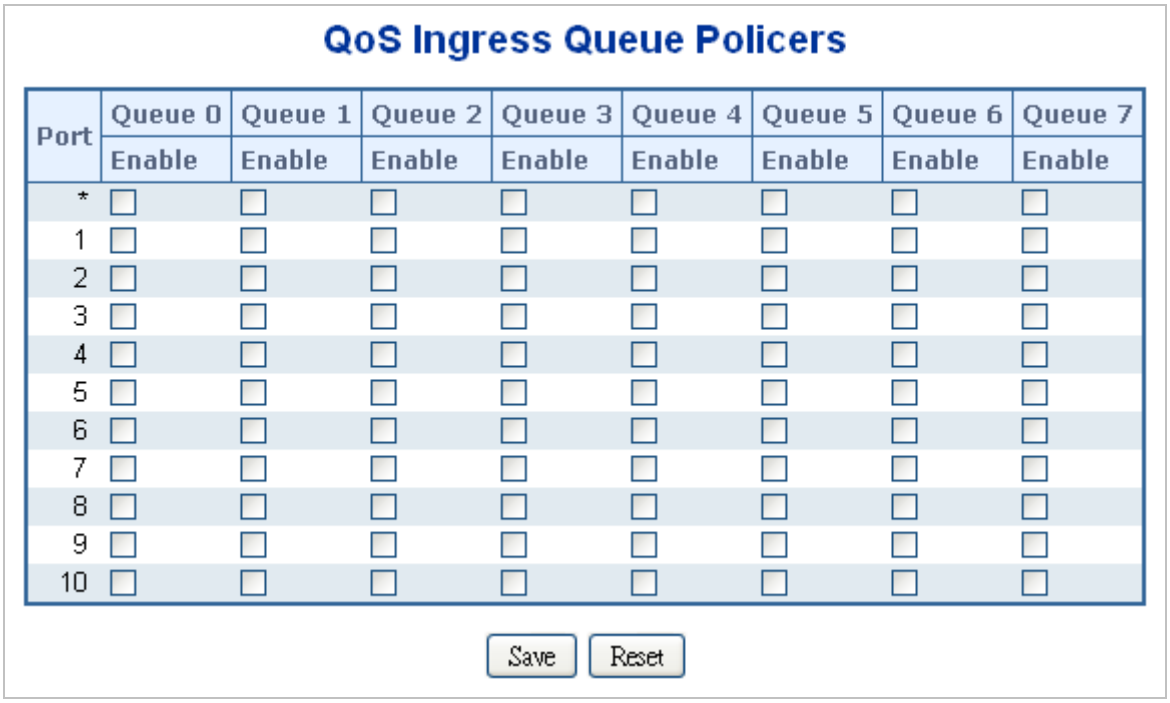


Figure 4-9-16: QoS Ingress Queue Policers Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Enable (E)**	Controls whether the queue policer is enabled on this switch port.
• **Rate**	Controls the rate for the queue policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps". This field is only shown if at least one of the queue policers is enabled.
• **Unit**	Controls the unit of measure for the queue policer rate as kbps or Mbps. The default value is "kbps". This field is only shown if at least one of the queue policers is enabled.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.9.14 Storm Control Configuration

Storm control for the switch is configured on this page.

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch. The Storm Control Configuration screen in Figure 4-9-17 appears.

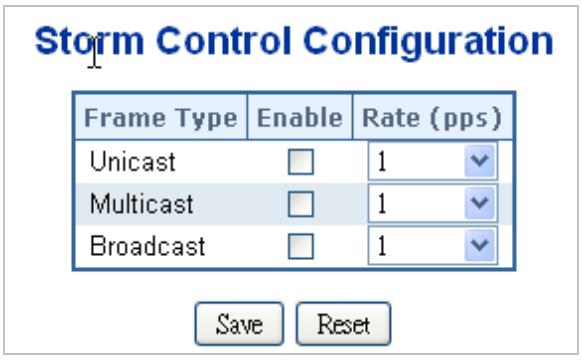


Figure 4-9-17: Storm Control Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Frame Type**	The settings in a particular row apply to the frame type listed here: ■ **unicast** ■ **multicast** ■ **Broadcast**
• **Enable**	Enable or disable the storm control status for the given frame type.
• **Rate**	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K.

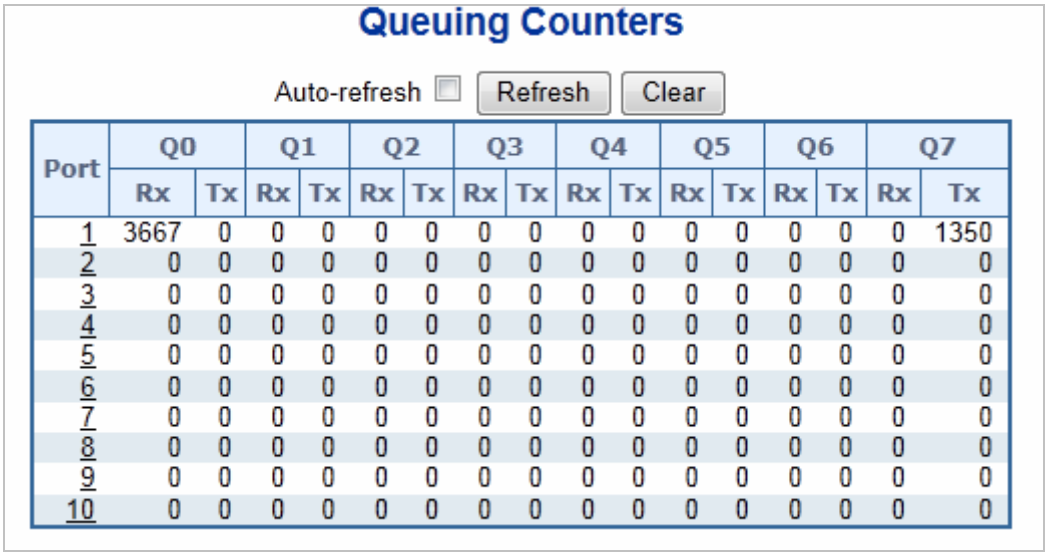
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.9.15 QoS Statistics

This page provides statistics for the different queues for all switch ports. The QoS Statistics screen in Figure 4-9-18 appears.



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	3667	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1350
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 4-9-18: Queuing Counters Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Q0 ~ Q7**	There are 8 QoS queues per port. Q0 is the lowest priority queue.
• **Rx/Tx**	The number of received and transmitted packets per queue.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

4.9.16 Voice VLAN Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI. The Voice VLAN Configuration screen in Figure 4-9-19 appears.

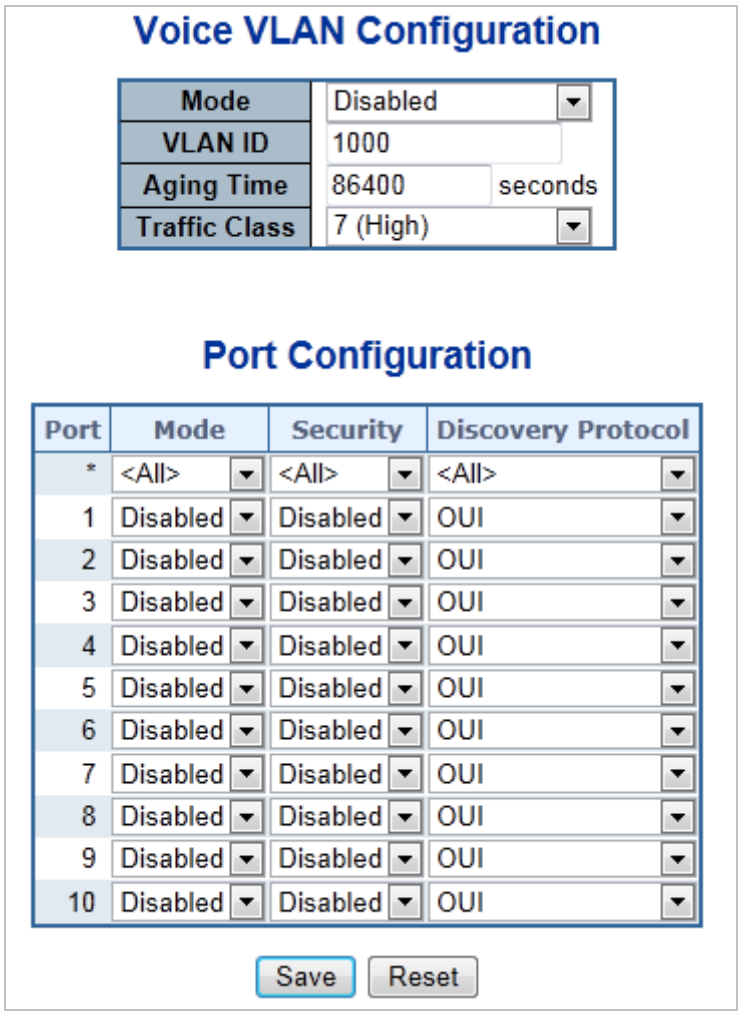


Figure 4-9-19: Voice VLAN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible modes are: ■ **Enabled**: Enable Voice VLAN mode operation. ■ **Disabled**: Disable Voice VLAN mode operation.
• **VLAN ID**	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is conflict configuration if the value equal management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.
• **Age Time**	Indicates the Voice VLAN secure learning age time. The allowed range is 10 to 10000000 seconds. It used when security mode or auto detect mode is enabled. In other cases, it will based hardware age time. The actual age time will be situated in the [age_time; 2 * age_time] interval.

• **Traffic Class**	Indicates the Voice VLAN traffic class. All traffic on Voice VLAN will apply this class.
• **Port Mode**	Indicates the Voice VLAN port mode. When the port mode isn't disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter. Possible port modes are: ■ **Disabled**: Disjoin from Voice VLAN. ■ **Auto**: Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configure the Voice VLAN members automatically. ■ **Forced**: Forced join to Voice VLAN. ■ **All** means all ports will have one specific setting.
• **Port Security**	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds. Possible port modes are: ■ **Enabled**: Enable Voice VLAN security mode operation. ■ **Disabled**: Disable Voice VLAN security mode operation. ■ **All** means all ports will have one specific setting.
• **Port Discovery Protocol**	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process? Possible discovery protocols are: ■ **OUI**: Detect telephony device by OUI address. ■ **LLDP**: Detect telephony device by LLDP. ■ **Both**: Both OUI and LLDP. ■ **All** means all ports will have one specific setting.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.9.17 Voice VLAN OUI Table

Configure VOICE VLAN OUI table on this page. The maximum entry number is 16. Modifying the OUI table will restart auto detection of OUI process. The Voice VLAN OUI Table screen in Figure 4-9-20 appears.

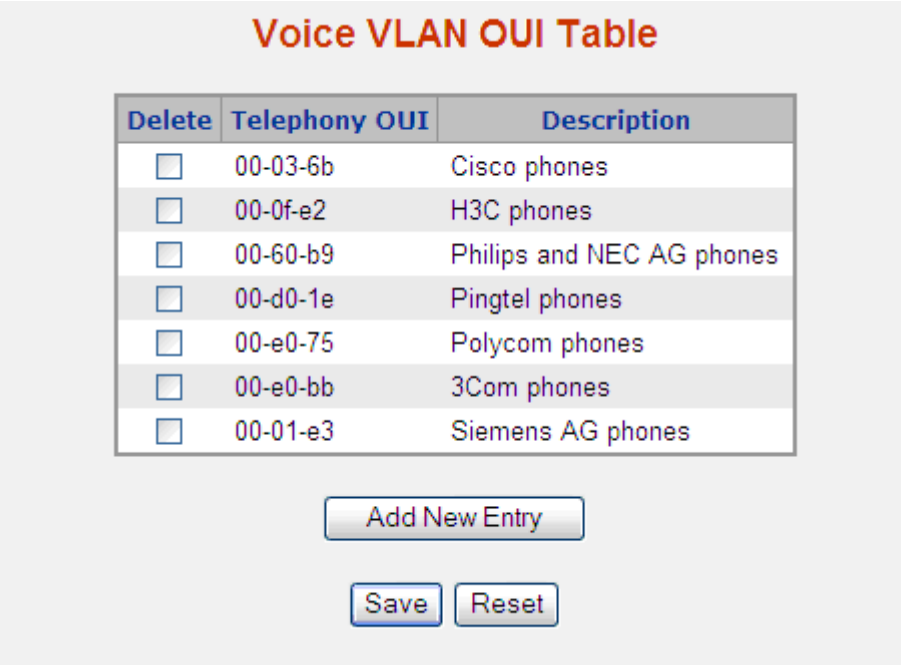


Figure 4-9-20 : Voice VLAN OUI Table Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Telephony OUI**	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
• **Description**	The description of OUI address. Normally, it descripts which vendor telephony device. The allowed string length is 0 to 32.

Buttons

Add New Entry: Click to add a new access management entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.10 Access Control Lists

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual

users or groups permitted or denied to specific traffic objects, such as a process or a program.
Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.
There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

4.10.1 Access Control List Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is **256** on each switch. The Voice VLAN OUI Table screen in Figure 4-10-1 appears.

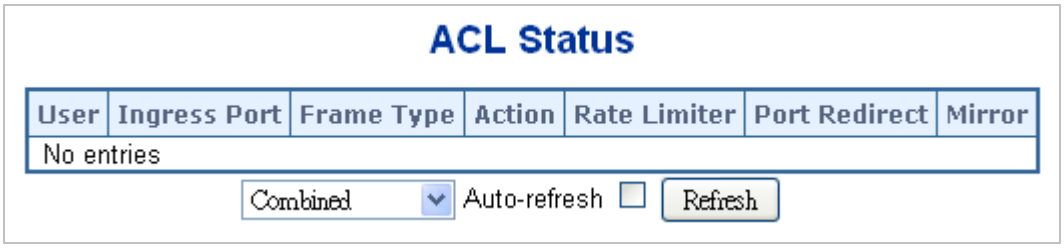


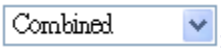
Figure 4-10-1: ACL Status Page Screenshot

The page includes the following fields:

Object	Description
• **User**	Indicates the ACL user.
• **Ingress Port**	Indicates the ingress port of the ACE. Possible values are: ■ **All**: The ACE will match all ingress port. ■ **Port**: The ACE will match a specific ingress port.
• **Frame Type**	Indicates the frame type of the ACE. Possible values are: ■ **Any**: The ACE will match any frame type. ■ **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ■ **ARP**: The ACE will match ARP/RARP frames. ■ **IPv4**: The ACE will match all IPv4 frames. ■ **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. ■ **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. ■ **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. ■ **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. ■ **IPv6**: The ACE will match all IPv6 standard frames.
• **Action**	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped.

• **Rate Limiter**	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
• **Port Redirect**	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are **Disabled** or a specific port number. When **Disabled** is displayed, the port redirect operation is disabled.
• **Mirror**	Specify the mirror operation of this port. The allowed values are: ■ **Enabled**: Frames received on the port are mirrored. ■ **Disabled**: Frames received on the port are not mirrored. The default value is **"Disabled"**.
• **CPU**	Forward packet that matched the specific ACE to CPU.
• **CPU Once**	Forward first packet that matched the specific ACE to CPU.
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.
• **Conflict**	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons



: Select the ACL status from this drop down list.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

: Click to refresh the page immediately.

4.10.2 Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is **256** on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

The Access Control List Configuration screen in Figure 4-10-2 appears.

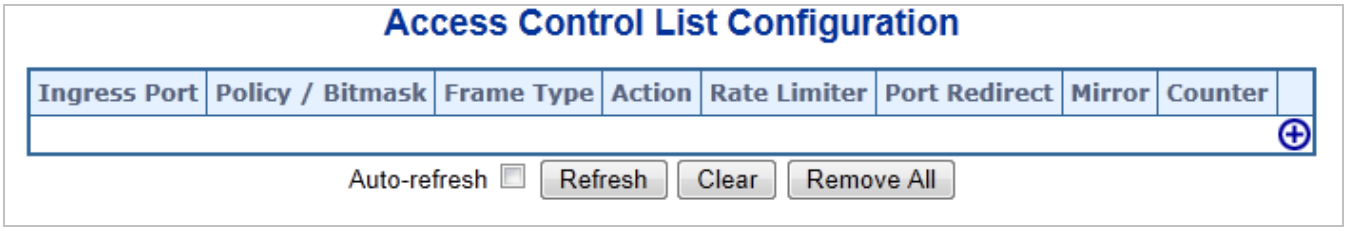


Figure 4-10-2: Access Control List Configuration Page Screenshot

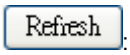
The page includes the following fields:

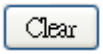
Object	Description
• **Ingress Port**	Indicates the ingress port of the ACE. Possible values are: ■ **All:** The ACE will match all ingress port. ■ **Port:** The ACE will match a specific ingress port.
• **Policy / Bitmask**	Indicates the policy number and bitmask of the ACE.
• **Frame Type**	Indicates the frame type of the ACE. Possible values are: ■ **Any**: The ACE will match any frame type. ■ **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ■ **ARP**: The ACE will match ARP/RARP frames. ■ **IPv4**: The ACE will match all IPv4 frames. ■ **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. ■ **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. ■ **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. ■ **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. ■ **IPv6**: The ACE will match all IPv6 standard frames.
• **Action**	Indicates the forwarding action of the ACE. ■ **Permit**: Frames matching the ACE may be forwarded and learned. ■ **Deny**: Frames matching the ACE are dropped.
• **Rate Limiter**	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
• **Port Redirect**	Indicates the ingress port of the ACE. Possible values are: ■ **All:** The ACE will match all ingress port. ■ **Port:** The ACE will match a specific ingress port.
• **Mirror**	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: ■ **Enabled:** Frames received on the port are mirrored. ■ **Disabled:** Frames received on the port are not mirrored. The default value is "Disabled".
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.

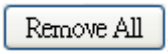
• **Modification Buttons**	You can modify each ACE (Access Control Entry) in the table using the following buttons: : Inserts a new ACE before the current row. : Edits the ACE row. : Moves the ACE up the list. : Moves the ACE down the list. : Deletes the ACE. : The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

 : Click to refresh the page immediately.

 : Click to clear the counters.

 : Click to remove all ACEs.

4.10.3 ACE Configuration

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here. The ACE Configuration screen in Figure 4-10-3 appears.

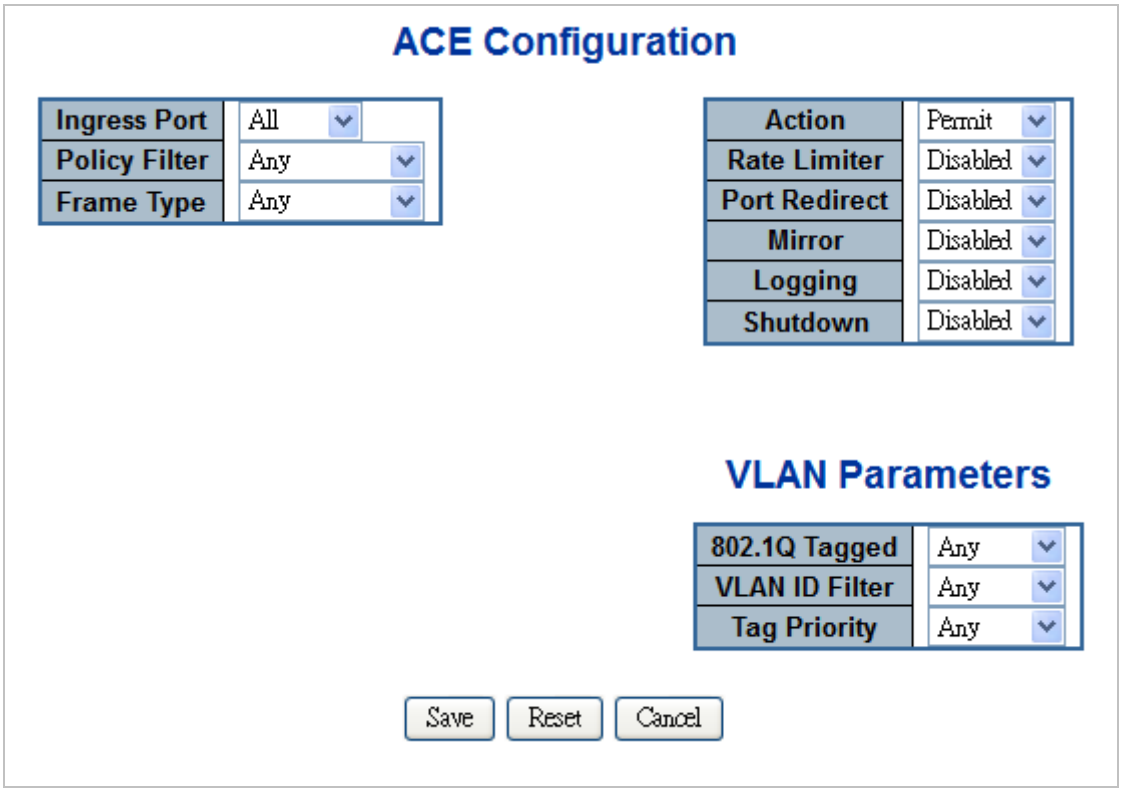


Figure 4-10-3: ACE Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Ingress Port**	Select the ingress port for which this ACE applies. ■ **All:** The ACE applies to all port. ■ **Port*n*:** The ACE applies to this port number, where *n* is the number of the switch port.
• **Policy Filter**	Specify the policy number filter for this ACE. ■ **Any:** No policy filter is specified. (policy filter status is "don't-care".) ■ **Specific:** If you want to filter a specific policy with this ACE, choose this value. Two field for entering a policy value and bitmask appears.
• **Policy Value**	When **"Specific"** is selected for the policy filter, you can enter a specific policy value. The allowed range is **0** to **255**.
• **Policy Bitmask**	When **"Specific"** is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is **0x0** to **0xff**.
• **Frame Type**	Select the frame type for this ACE. These frame types are mutually exclusive. ■ **Any**: Any frame can match this ACE.

	■ **Ethernet Type**: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ■ **ARP**: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type. ■ **IPv4**: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.
• **Action**	Specify the action to take with a frame that hits this ACE. ■ **Permit**: The frame that hits this ACE is granted permission for the ACE operation. ■ **Deny**: The frame that hits this ACE is dropped.
• **Rate Limiter**	Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.
• **EVC Policer**	Select whether EVC policer is enabled or disabled. The default value is **"Disabled"**.
• **EVC Policer ID**	Select which EVC policer ID to apply on this ACE. The allowed values are **Disabled** or the values **1** through **128**.
• **Port Redirect**	Frames that hit the ACE are redirected to the port number specified here. The allowed range is the same as the switch port number range. **Disabled** indicates that the port redirect operation is disabled.
• **Mirror**	Specify the mirror operation of this port. The allowed values are: ■ **Enabled**: Frames received on the port are mirrored. ■ **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".
• **Logging**	Specify the logging operation of the ACE. The allowed values are: ■ **Enabled**: Frames matching the ACE are stored in the System Log. ■ **Disabled**: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
• **Shutdown**	Specify the port shut down operation of the ACE. The allowed values are: ■ **Enabled**: If a frame matches the ACE, the ingress port will be disabled. ■ **Disabled**: Port shut down is disabled for the ACE.
• **Counter**	The counter indicates the number of times the ACE was hit by a frame.

■ MAC Parameters

Object	Description
• **SMAC Filter**	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. ■ **Any**: No SMAC filter is specified. (SMAC filter status is "don't-care".) ■ **Specific**: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
• **SMAC Value**	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.
• **DMAC Filter**	Specify the destination MAC filter for this ACE. ■ **Any**: No DMAC filter is specified. (DMAC filter status is "don't-care".) ■ **MC**: Frame must be multicast. ■ **BC**: Frame must be broadcast. ■ **UC**: Frame must be unicast. ■ **Specific**: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
• **DMAC Value**	When **"Specific"** is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.

■ VLAN Parameters

Object	Description
• **802.1Q Tagged**	Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are: ■ **Any**: Any value is allowed ("don't-care"). ■ **Enabled**: Tagged frame only. ■ **Disabled**: Untagged frame only. The default value is "Any".
• **VLAN ID Filter**	Specify the VLAN ID filter for this ACE. ■ **Any**: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) ■ **Specific**: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
• **VLAN ID**	When **"Specific"** is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
• **Tag Priority**	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

■ ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

Object	Description
• **ARP/RARP**	Specify the available ARP/RARP opcode (OP) flag for this ACE. ■ **Any**: No ARP/RARP OP flag is specified. (OP is "don't-care".) ■ **ARP**: Frame must have ARP/RARP opcode set to ARP. ■ **RARP**: Frame must have ARP/RARP opcode set to RARP. ■ **Other**: Frame has unknown ARP/RARP Opcode flag.
• **Request/Reply**	Specify the available ARP/RARP opcode (OP) flag for this ACE. ■ **Any**: No ARP/RARP OP flag is specified. (OP is "don't-care".) ■ **Request**: Frame must have ARP Request or RARP Request OP flag set. ■ **Reply**: Frame must have ARP Reply or RARP Reply OP flag.
• **Sender IP Filter**	Specify the sender IP filter for this ACE. ■ **Any**: No sender IP filter is specified. (Sender IP filter is "don't-care".) ■ **Host**: Sender IP filter is set to Host. Specify the sender IP address in

	the SIP Address field that appears. ■ **Network**: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
• **Sender IP Address**	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
• **Sender IP Mask**	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
• **Target IP Filter**	Specify the target IP filter for this specific ACE. ■ **Any**: No target IP filter is specified. (Target IP filter is "don't-care".) ■ **Host**: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. ■ **Network**: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.
• **Target IP Address**	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
• **Target IP Mask**	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
• **ARP SMAC Match**	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. ■ **0**: ARP frames where SHA is not equal to the SMAC address. ■ **1**: ARP frames where SHA is equal to the SMAC address. ■ **Any**: Any value is allowed ("don't-care").
• **RARP SMAC Match**	Specify whether frames can hit the action according to their target hardware address field (THA) settings. ■ **0**: RARP frames where THA is not equal to the SMAC address. ■ **1**: RARP frames where THA is equal to the SMAC address. ■ **Any**: Any value is allowed ("don't-care").
• **IP/Ethernet Length**	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. ■ **0**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). ■ **1**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). ■ **Any**: Any value is allowed ("don't-care").
• **IP**	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. ■ **0**: ARP/RARP frames where the HLD is equal to Ethernet (1). ■ **1**: ARP/RARP frames where the HLD is equal to Ethernet (1). ■ **Any**: Any value is allowed ("don't-care").
• **Ethernet**	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings. ■ **0**: ARP/RARP frames where the PRO is equal to IP (0x800). ■ **1**: ARP/RARP frames where the PRO is equal to IP (0x800). ■ **Any**: Any value is allowed ("don't-care").

■ IP Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

Object	Description
• **IP Protocol Filter**	Specify the IP protocol filter for this ACE. ■ **Any**: No IP protocol filter is specified ("don't-care"). ■ **Specific**: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears. ■ **ICMP**: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. ■ **UDP**: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. ■ **TCP**: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.

• **IP Protocol Value**	When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IP protocol value.
• **IP TTL**	Specify the Time-to-Live settings for this ACE. ■ **zero**: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. ■ **non-zero**: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. ■ **Any**: Any value is allowed ("don't-care").
• **IP Fragment**	Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. ■ **No**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. ■ **Yes**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. ■ **Any**: Any value is allowed ("don't-care").
• **IP Option**	Specify the options flag setting for this ACE. ■ **No**: IPv4 frames where the options flag is set must not be able to match this entry. ■ **Yes**: IPv4 frames where the options flag is set must be able to match this entry. ■ **Any**: Any value is allowed ("don't-care").
• **SIP Filter**	Specify the source IP filter for this ACE. ■ **Any**: No source IP filter is specified. (Source IP filter is "don't-care".) ■ **Host**: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. ■ **Network**: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.
• **SIP Address**	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
• **SIP Mask**	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
• **DIP Filter**	Specify the destination IP filter for this ACE. ■ **Any**: No destination IP filter is specified. (Destination IP filter is "don't-care".) ■ **Host**: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. ■ **Network**: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.
• **DIP Address**	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
• **DIP Mask**	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

■ ICMP Parameters

Object	Description
• **ICMP Type Filter**	Specify the ICMP filter for this ACE. ■ **Any**: No ICMP filter is specified (ICMP filter status is "don't-care"). ■ **Specific**: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.
• **ICMP Type Value**	When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is **0** to **255**. A frame that hits this ACE matches this ICMP value.
• **ICMP Code Filter**	Specify the ICMP code filter for this ACE. ■ **Any**: No ICMP code filter is specified (ICMP code filter status is "don't-care"). ■ **Specific**: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

• **ICMP Code Value**	When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is **0** to **255**. A frame that hits this ACE matches this ICMP code value.

■ TCP/UDP Parameters

Object	Description
• **TCP/UDP Source Filter**	Specify the TCP/UDP source filter for this ACE. ■ **Any**: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). ■ **Specific**: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. ■ **Range**: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.
• **TCP/UDP Source No.**	When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.
• **TCP/UDP Source Range**	When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.
• **TCP/UDP Destination Filter**	Specify the TCP/UDP destination filter for this ACE. ■ **Any**: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). ■ **Specific**: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. ■ **Range**: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.
• **TCP/UDP Destination Number**	When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.
• **TCP/UDP Destination Range**	When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.
• **TCP FIN**	Specify the TCP "No more data from sender" (FIN) value for this ACE. ■ **0**: TCP frames where the FIN field is set must not be able to match this entry. ■ **1**: TCP frames where the FIN field is set must be able to match this entry. ■ **Any**: Any value is allowed ("don't-care").
• **TCP SYN**	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. ■ **0**: TCP frames where the SYN field is set must not be able to match this entry. ■ **1**: TCP frames where the SYN field is set must be able to match this entry. ■ **Any**: Any value is allowed ("don't-care").
• **TCP RST**	Specify the TCP "Reset the connection" (RST) value for this ACE. ■ **0**: TCP frames where the RST field is set must not be able to match this entry. ■ **1**: TCP frames where the RST field is set must be able to match this entry. ■ **Any**: Any value is allowed ("don't-care").
• **TCP PSH**	Specify the TCP "Push Function" (PSH) value for this ACE. ■ **0**: TCP frames where the PSH field is set must not be able to match this entry. ■ **1**: TCP frames where the PSH field is set must be able to match this entry. ■ **Any**: Any value is allowed ("don't-care").
• **TCP ACK**	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. ■ **0**: TCP frames where the ACK field is set must not be able to match this entry. ■ **1**: TCP frames where the ACK field is set must be able to match this entry.

	■ **Any**: Any value is allowed ("don't-care").
• **TCP URG**	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. ■ **0**: TCP frames where the URG field is set must not be able to match this entry. ■ **1**: TCP frames where the URG field is set must be able to match this entry. ■ **Any**: Any value is allowed ("don't-care").

■ Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

Object	Description
• **EtherType Filter**	Specify the Ethernet type filter for this ACE. ■ **Any**: No EtherType filter is specified (EtherType filter status is "don't-care"). ■ **Specific**: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering an EtherType value appears.
• **Ethernet Type Value**	When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is **0x600** to **0xFFFF** but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD (IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

Save: Click to save changes.

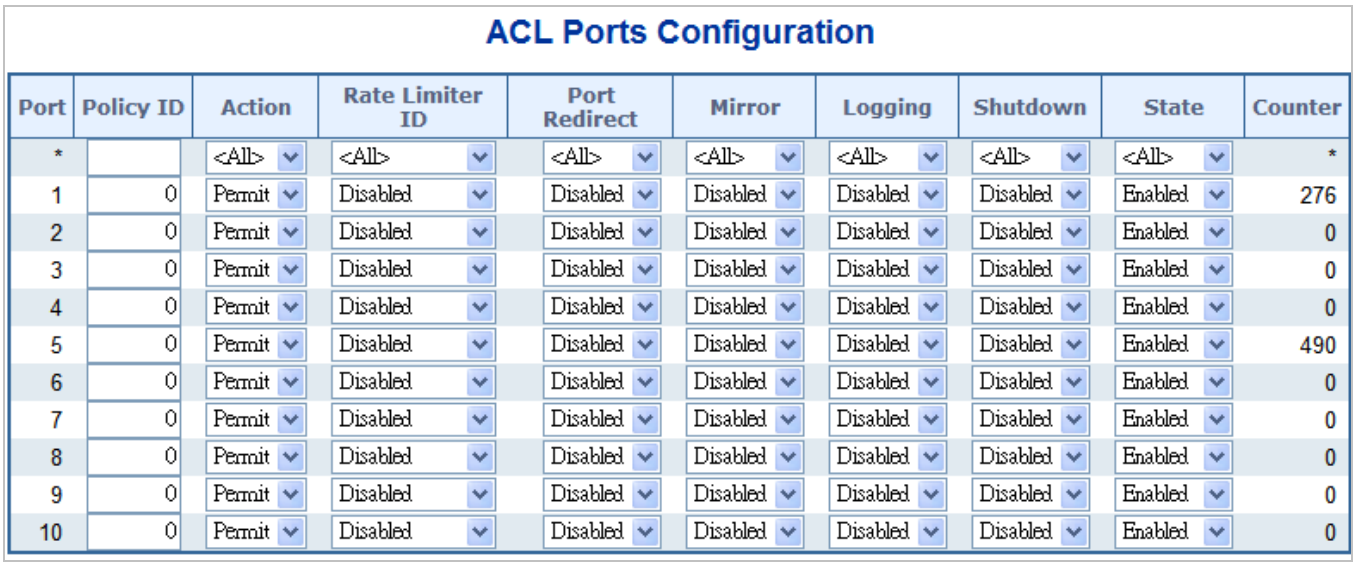
Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Return to the previous page.

4.10.4 ACL Ports Configuration

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

The ACL Ports Configuration screen in Figure 4-10-4 appears.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*		<All>	<All>	<All>	<All>	<All>	<All>	<All>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	276
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	490
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0

Figure 4-10-4: ACL Ports Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings contained in the same row.
• **Policy ID**	Select the policy to apply to this port. The allowed values are **1** through **8**. The default value is **1**.
• **Action**	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is **"Permit"**. **All** means all ports will have one specific setting.
• **Rate Limiter ID**	Select which rate limiter to apply to this port. The allowed values are **Disabled** or the values **1** through **15**. The default value is **"Disabled"**. **All** means all ports will have one specific setting.
• **Port Redirect**	Select which port frames are redirected on. The allowed values are **Disabled** or a specific port number. The default value is **"Disabled"**. **All** means all ports will have one specific setting.
• **Mirror**	Specify the mirror operation of this port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is **"Disabled".** **All** means all ports will have one specific setting.
• **Logging**	Specify the logging operation of this port. The allowed values are: **Enabled**: Frames received on the port are stored in the System Log. **Disabled**: Frames received on the port are not logged. The default value is **"Disabled"**. Please note that the System Log memory size and logging rate is limited. **All** means all ports will have one specific setting.
• **Shutdown**	Specify the port shut down operation of this port. The allowed values are: **Enabled**: If a frame is received on the port, the port will be disabled. **Disabled**: Port shut down is disabled. The default value is **"Disabled"**. **All** means all ports will have one specific setting.
• **State**	Specify the port state of this port. The allowed values are: **Enabled**: To reopen ports by changing the volatile port configuration of the ACL user module. **Disabled**: To close ports by changing the volatile port configuration of the ACL user module. The default value is **"Enabled"**. **All** means all ports will have one specific setting.
• **Counter**	Counts the number of frames that match this ACE.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the counters.

4.10.5 ACL Rate Limiter Configuration

Configure the rate limiter for the ACL of the switch.

The ACL Rate Limiter Configuration screen in Figure 4-10-5 appears.

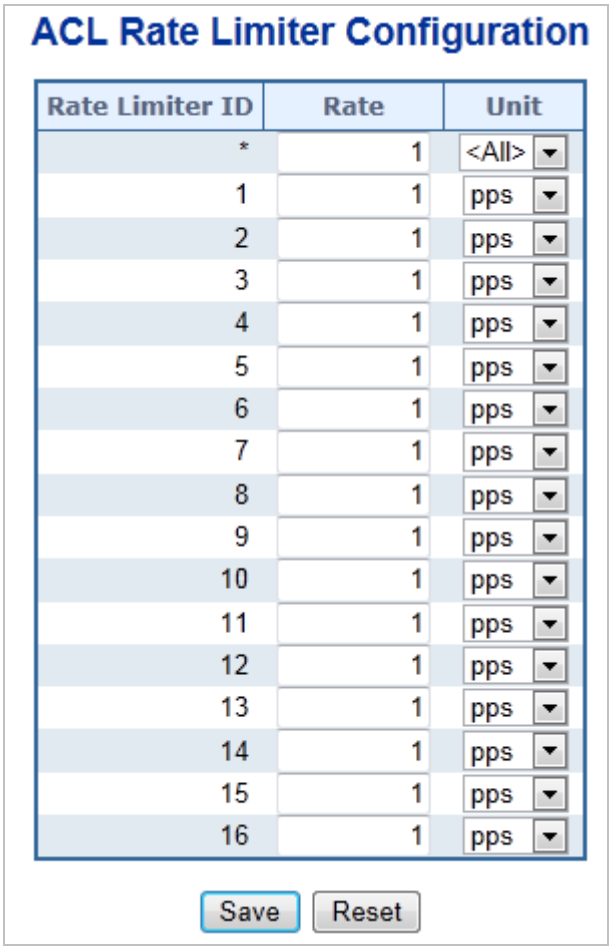


Figure 4-10-5: ACL Rate Limiter Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Rate Limiter ID**	The rate limiter ID for the settings contained in the same row.

• **Rate**	The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.
• **Unit**	Specify the rate unit. The allowed values are: ■ **pps**: packets per second. ■ **kbps**: Kbits per second. **All** means all ports will have one specific setting.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.11 Authentication

This section is to control the access of the Managed Switch, includes the user access and management control.
The Authentication section contains links to the following main topics:

- **IEEE 802.1X Port-Based Network Access Control**
- **MAC-Based Authentication**
- **User Authentication**

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch is special 802.1X frames, known as **EAPOL (EAP Over LANs)** frames. EAPOL frames encapsulate **EAP PDU**s (RFC3748). Frames sent between the switch and the RADIUS server is RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like **MD5-Challenge**, **PEAP**, and **TLS**. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is

a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide.

Overview of User Authentication

It is allowed to configure the Managed Switch to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and Web browser. This Managed Switch provides secure network management access using the following options:

- **Remote Authentication Dial-in User Service (RADIUS)**
- **Terminal Access Controller Access Control System Plus (TACACS+)**
- **Local user name and Priviledge Level control**

RADIUS and TACACS+ are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An **authentication server** contains a database of multiple user name / password pairs with associated privilege levels for each user that requires management access to the Managed Switch.

4.11.1 Understanding IEEE 802.1X Port-Based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only **Extensible Authentication Protocol over LAN (EAPOL)** traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ **Device Roles**

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.

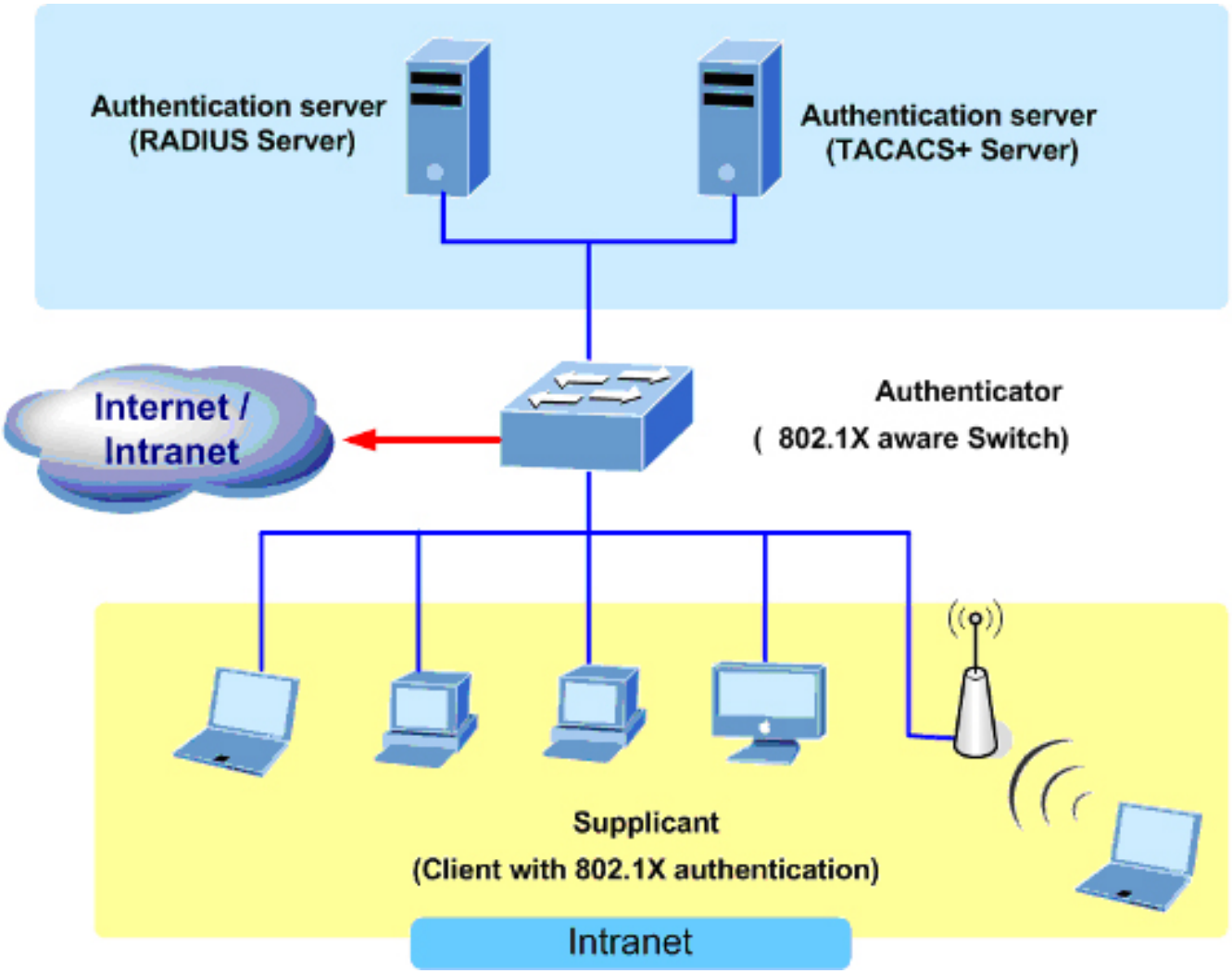


Figure 4-11-1

- ***Client***—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1X specification.)

- ***Authentication server***—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible Authentication Protocol (EAP)** extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- ***Switch* (802.1X device)**—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ **Authentication Initiation and Message Exchange**

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during boot up, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity

If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port was in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. “Figure 4-11-2” shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

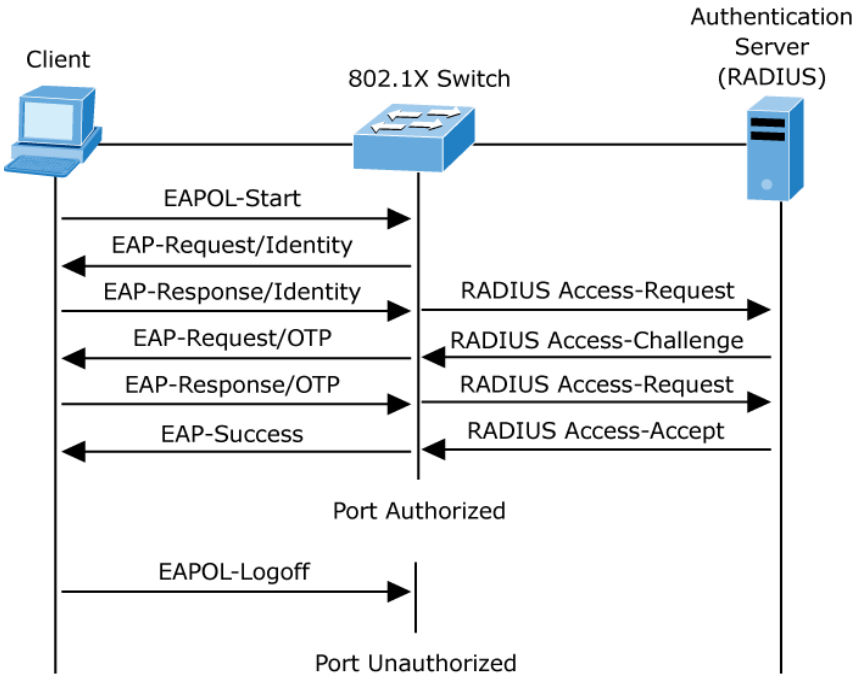


Figure 4-11-2: EAP Message Exchange

■ **Ports in Authorized and Unauthorized States**

The switch port state determines whether or not the client is granted access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

4.11.2 Authentication Configuration

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces. The Authentication Method Configuration screen in Figure 4-11-3 appears.

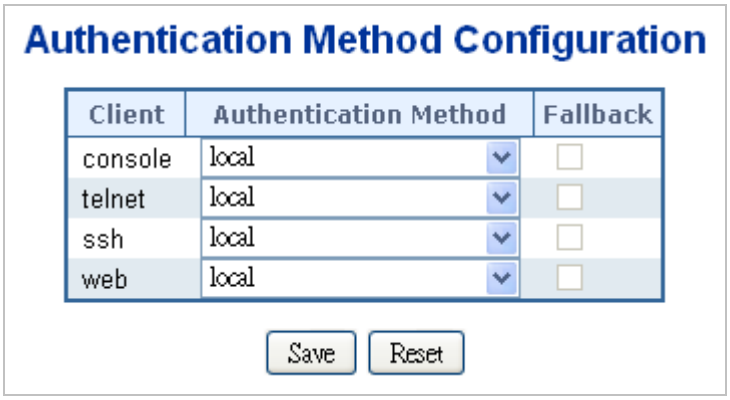


Figure 4-11-3: Authentication Method Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Client**	The management client for which the configuration below applies.
• **Authentication Method**	Authentication Method can be set to one of the following values: ■ **None**: authentication is disabled and login is not possible. ■ **local**: use the local user database on the switch stack for authentication. ■ **RADIUS**: use a remote RADIUS server for authentication. ■ **TACACSt+**: use a remote TACACS+ server for authentication.
• **Fallback**	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to something else than 'none or 'local'.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.11.3 Network Access Server Configuration

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.
The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1 X authentications. The NAS configuration consists of two sections, a system- and a port-wide. The Network Access Server Configuration screen in Figure 4-11-4 appears.

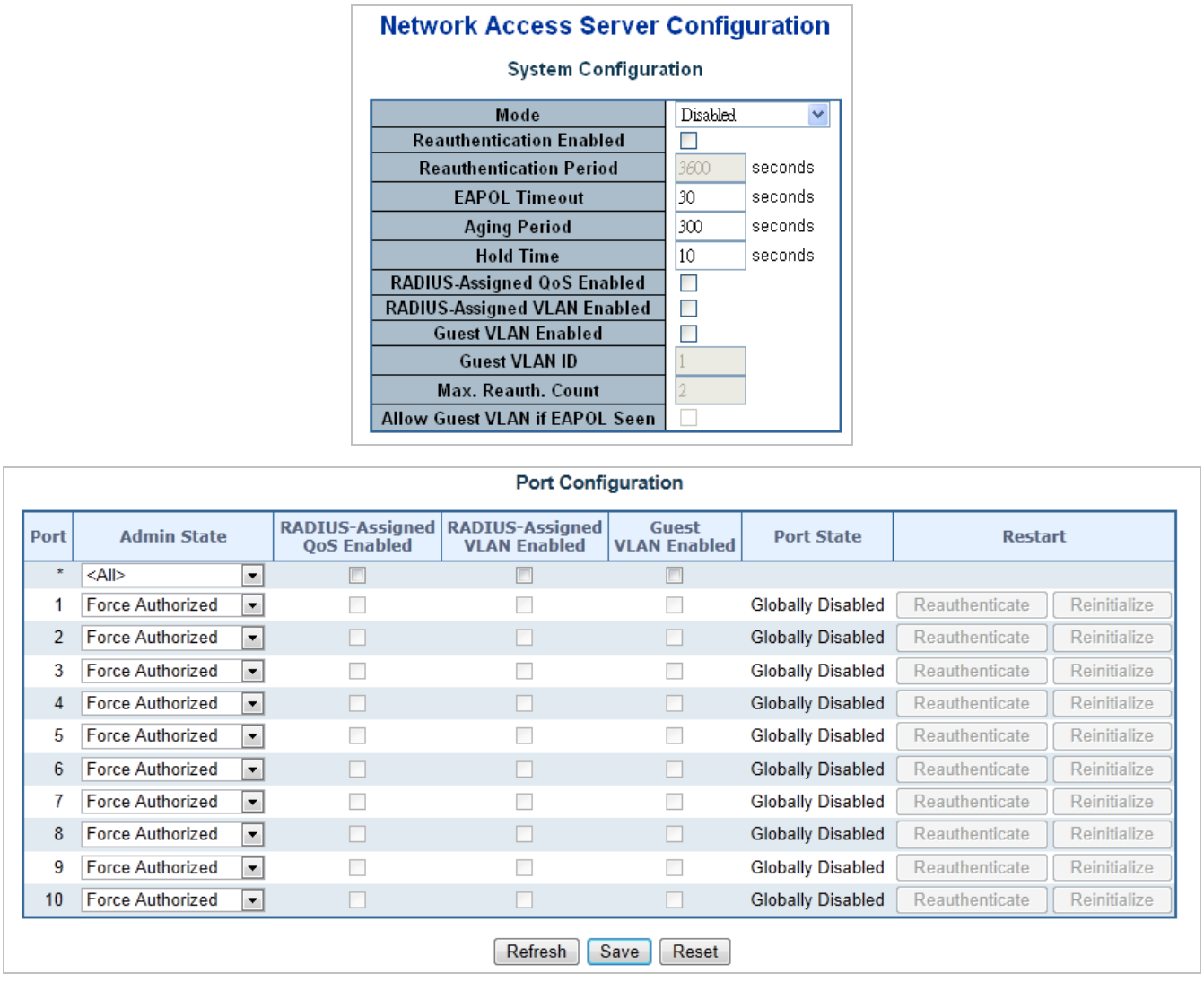


Figure 4-11-4: Network Access Server Configuration Page Screenshot

The page includes the following fields:

System Configuration

Object	Description
• **Mode**	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
• **Reauthentication Enabled**	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port.
• **Reauthentication Period**	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
• **EAPOL Timeout**	Determines the time between retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
• **Aging Period**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: ■ **Single 802.1X** ■ **Multi 802.1X** ■ **MAC-Based Auth**. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in a 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
• **Hold Time**	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: ■ **Single 802.1X** ■ **Multi 802.1X** ■ **MAC-Based Auth**. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
• **RADIUS-Assigned QoS Enabled**	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled for that port. When unchecked, RADIUS-server assigned QoS

	Class is disabled for all ports.
• **RADIUS-Assigned VLAN Enabled**	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled for that port. When unchecked, RADIUS-server assigned VLAN is disabled for all ports.
• **Guest VLAN Enabled**	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled for all ports.
• **Guest VLAN ID**	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].
• **Max. Reauth. Count**	The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
• **Allow Guest VLAN if EAPOL Seen**	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Admin State**	The Configuration All with available options will assign to whole ports. If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication. **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access. **Port-based 802.1X** In the 802.1X-world, the user is called the supplicant, the switch is the

authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch is special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.
When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.
Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.
Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.
Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.
In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants

	are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality. **MAC-based Auth.** Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1 X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.
• **RADIUS-Assigned QoS Enabled**	When RADIUS-Assigned QoS is both globally enabled and enabled (checked) for a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • **Port-based 802.1X** • **Single 802.1X** **RADIUS attributes used in identifying a QoS Class:** Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule: All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3].
• **RADIUS-Assigned VLAN Enabled**	When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the

	RADIUS-assigned). This option is only available for single-client modes, i.e. • **Port-based 802.1X** • **Single 802.1X** For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. **RADIUS attributes used in identifying a VLAN ID:** RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used: - The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. - The switch looks for the first set of these attributes that have the same Tag value and fulfill the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].
• **Guest VLAN Enabled**	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.: • **Port-based 802.1X** • **Single 802.1X** • **Multi 802.1X** For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. **Guest VLAN Operation:** When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile; the switch considers entering the Guest VLAN. The interval between transmissions of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.
• **Port State**	The current state of the port. It can undertake one of the following values: ■ **Globally Disabled**: NAS is globally disabled. ■ **Link Down**: NAS is globally enabled, but there is no link on the port. ■ **Authorized**: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. ■ **Unauthorized**: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. ■ **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X

	clients are authorized and Y is unauthorized.
• **Restart**	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. **Reauthenticate**: Schedules a reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized. **Reinitialize**: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons

Refresh: Click to refresh the page.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.11.4 Network Access Overview

This page provides an overview of the current NAS port states for the selected switch. The Network Access Overview screen in Figure 4-11-5 appears.

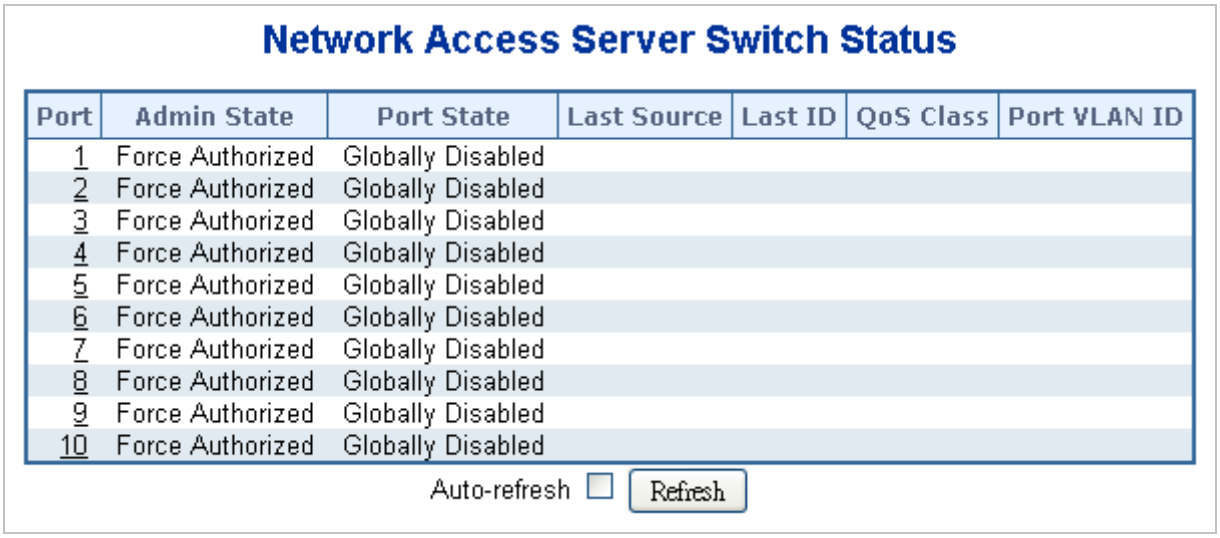


Figure 4-11-5: Network Access Server Switch Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number. Click to navigate to detailed NAS statistics for this port.
• **Admin State**	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
• **Port State**	The current state of the port. Refer to NAS Port State for a description of the individual states.
• **Last Source**	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
• **Last ID**	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
• **QoS Class**	QoS Class assigned to the port by the RADIUS server if enabled.
• **Port VLAN ID**	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.11.5 Network Access Statistics

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed. The Network Access Statistics screen in Figure 4-11-6 appears.

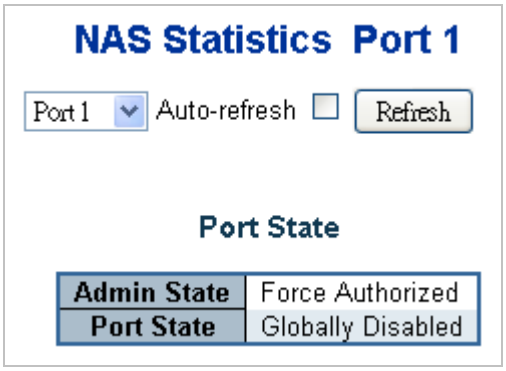


Figure 4-11-6: Network Access Statistics Page Screenshot

The page includes the following fields:

Port State

Object	Description
• **Admin State**	The port's current administrative state. Refer to NAS Admin State for a description

	of possible values.
• **Port State**	The current state of the port. Refer to NAS Port State for a description of the individual states.
• **QoS Class**	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
• **Port VLAN ID**	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Port Counters

Object	Description
• **EAPOL Counters**	These supplicant frame counters are available for the following administrative states: **Force Authorized** **Force Unauthorized** **Port-based 802.1X** **Single 802.1X** **Multi 802.1X**

Direction	Name	IEEE Name	Description
Rx	**Total**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that has been received by the switch.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	**Logoff**	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	**Invalid Length**	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	**Total**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that has been transmitted by the switch.

	Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
	Tx	**Requests**	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

- **Backend Server Counters**

These backend (RADIUS) frame counters are available for the following administrative states:

- **Port-based 802.1X**
- **Single 802.1X**
- **Multi 802.1X**
- **MAC-based Auth**.

Direction	Name	IEEE Name	Description
Rx	**Access Challenges**	dot1xAuthBackendAccessChallenges	**802.1X-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	**Other Requests**	dot1xAuthBackendOtherRequestsToSupplicant	**802.1X-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable.
Rx	**Auth. Successes**	dot1xAuthBackendAuthSuccesses	**802.1X- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	**Auth. Failures**	dot1xAuthBackendAuthFails	**802.1X- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	**Responses**	dot1xAuthBackendResponses	**802.1X-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the

		backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.
• **Last Supplicant/Client Info**	Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states: **Port-based 802.1X** **Single 802.1X** **Multi 802.1X** **MAC-based Auth**.	

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable.
Identity	-	**802.1X-based**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based**: Not applicable.

Selected Counters

Object	Description
• **Selected Counters**	The Selected Counters table is visible when the port is one of the following administrative states: ■ **Multi 802.1X** ■ **MAC-based Auth**. The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC Address

Object	Description
• **Identity**	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached. This column is not available for MAC-based Auth.
• **MAC Address**	For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.
• **VLAN ID**	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.
• **State**	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
• **Last Authentication**	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: This button is available in the following modes:

• Force Authorized

• Force Unauthorized

• Port-based 802.1X

• Single 802.1X

Click to clear the counters for the selected port.

Clear All: This button is available in the following modes:

• Multi 802.1X

• MAC-based Auth.X

Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared,

however.

: This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Click to clear only the currently selected client's counters.

4.11.6 Authentication Server Configuration

This page allows you to configure the Authentication Servers. The Authentication Server Configuration screen in Figure 4-11-7 appears.

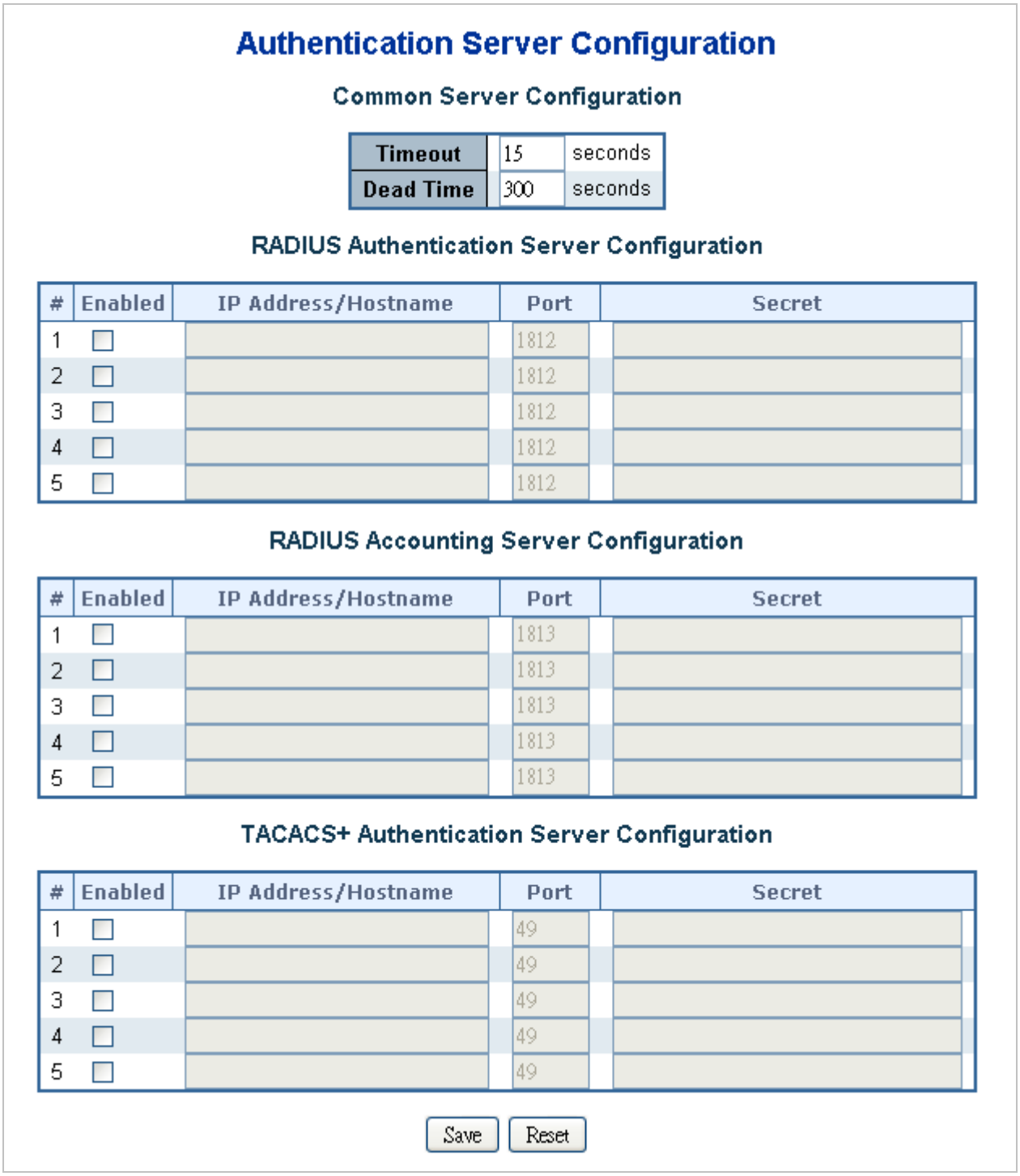


Figure 4-11-7: Authentication Server Configuration Page Screenshot

The page includes the following fields:

Port State

These settings are common for all of the Authentication Servers.

Object	Description
• **Timeout**	The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
• **Dead Time**	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

Object	Description
• #	The RADIUS Authentication Server number for which the configuration below applies.
• **Enabled**	Enable the RADIUS Authentication Server by checking this box.
• **IP Address/Hostname**	The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
• **Port**	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
• **Secret**	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.

RADIUS Accounting Server Configuration

The table has one row for each RADIUS Accounting Server and a number of columns, which are:

Object	Description
• #	The RADIUS Accounting Server number for which the configuration below applies.
• **Enabled**	Enable the RADIUS Accounting Server by checking this box.
• **IP Address/Hostname**	The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.
• **Port**	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0

	(zero), the default port (1813) is used on the RADIUS Accounting Server.
• **Secret**	The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch.

TACACS+ Authentication Server Configuration

The table has one row for each TACACS+ Authentication Server and a number of columns, which are:

Object	Description
• #	The TACACS+ Authentication Server number for which the configuration below applies.
• **Enabled**	Enable the TACACS+ Authentication Server by checking this box.
• **IP Address/Hostname**	The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.
• **Port**	The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.
• **Secret**	The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.11.7 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page. The RADIUS Authentication/Accounting Server Overview screen in Figure 4-11-8 appears.

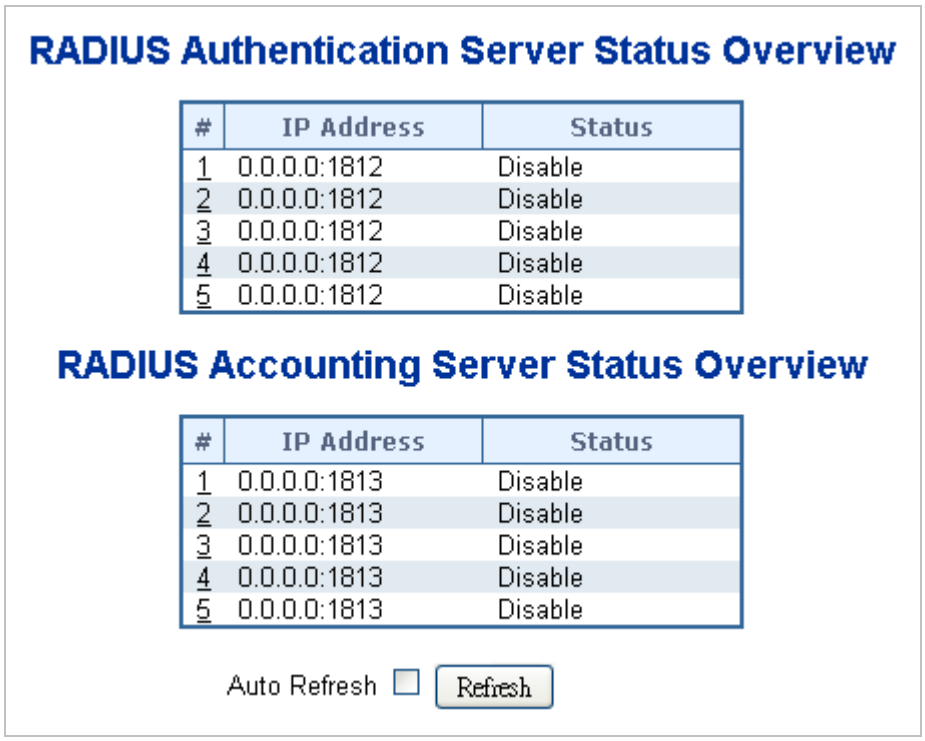


Figure 4-11-8: RADIUS Authentication/Accounting Server Overview Page Screenshot

The page includes the following fields:

RADIUS Authentication Server

Object	Description
• #	The RADIUS server number. Click to navigate to detailed statistics for this server.
• **IP Address**	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
• **Status**	The current state of the server. This field takes one of the following values: ■ **Disabled**: The server is disabled. ■ **Not Ready**: The server is enabled, but IP communication is not yet up and running. ■ **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. ■ **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Server

Object	Description
• #	The RADIUS server number. Click to navigate to detailed statistics for this server.
• **IP Address**	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
• **Status**	The current state of the server. This field takes one of the following values: ■ **Disabled**: The server is disabled.

	■ **Not Ready**: The server is enabled, but IP communication is not yet up and running. ■ **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.11.8 RADIUS Details

This page provides detailed statistics for a particular RADIUS server. The RADIUS Authentication/Accounting for Server Overview screen in Figure 4-11-9 appears.

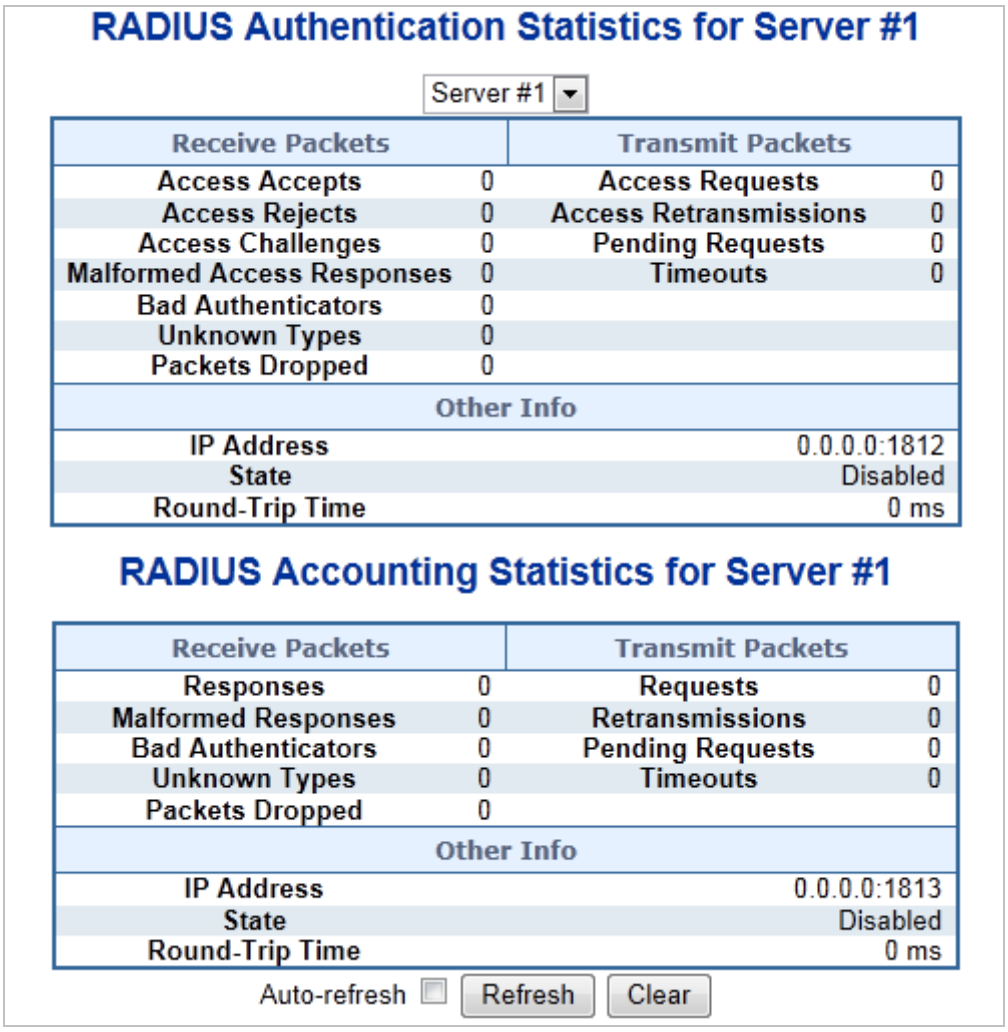


Figure 4-11-9: RADIUS Authentication/Accounting for Server Overview Page Screenshot

The page includes the following fields:

RADIUS Authentication Servers

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

Object	Description			
• **Packet Counters**	RADIUS authentication server packet counter. There are seven receive and four transmit counters.			
	Direction	**Name**	**RFC4668 Name**	**Description**
	Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
	Rx	**Access Rejects**	radiusAuthClientExtA	The number of RADIUS Access-Reject packets (valid

			ccessRejects	or invalid) received from the server.
	Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
	Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
	Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
	Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
	Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
	Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
	Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a

different server is counted as a Request as well as a timeout.

- **Other Info**

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Servers

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.

Use the server select box to switch between the backend servers to show details for.

Object	Description
• **Packet Counters**	RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Rx	**Responses**	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	**Malformed Responses**	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	**Unknown Types**	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.

	Rx	**Packets Dropped**	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
	Tx	**Requests**	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
	Tx	**Retransmissions**	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
	Tx	**Pending Requests**	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
	Tx	**Timeouts**	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

- **Other Info**

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running and the RADIUS module is ready to accept accounting attempts. **Dead (X seconds left)**: Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

4.11.9 Windows Platform RADIUS Server Configuration

Setup the RADIUS server and assign the client IP address to the Managed switch. In this case, field in the default IP Address of the Managed Switch with 192.168.0.100. And also make sure the shared **secret key** is as same as the one you had set at the Managed Switch's 802.1x system configuration – **12345678** at this case.

1. Configure the IP Address of remote RADIUS server and secret key.

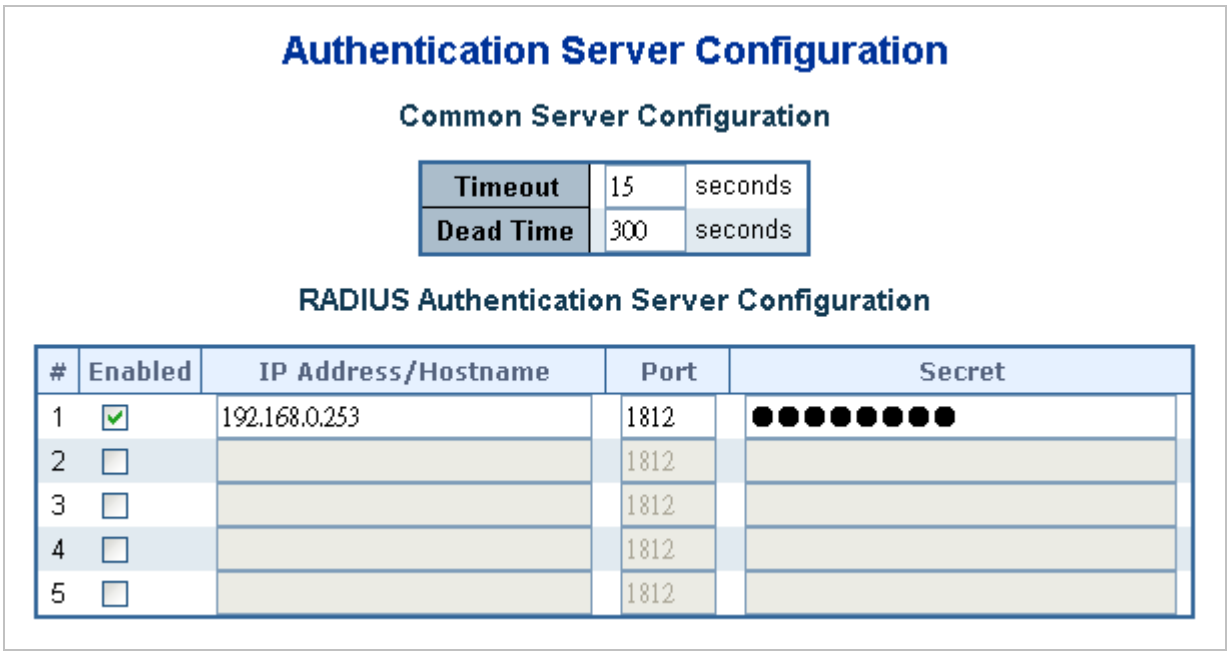


Figure 4-11-10: RADIUS Server Configuration Screenshot

2. Add New RADIUS Client on the Windows 2003 server

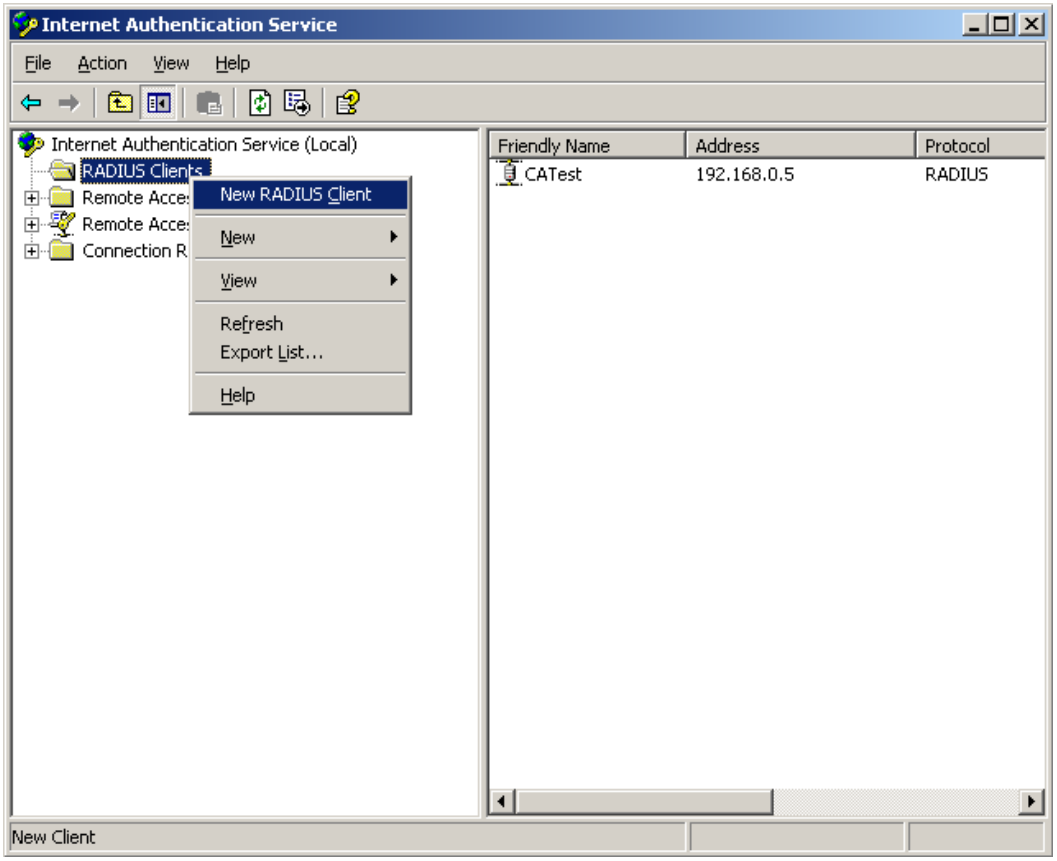


Figure 4-11-11: Windows Server – Add New RADIUS Client Setting

3. Assign the client IP address to the **Industrial Managed Switch**.

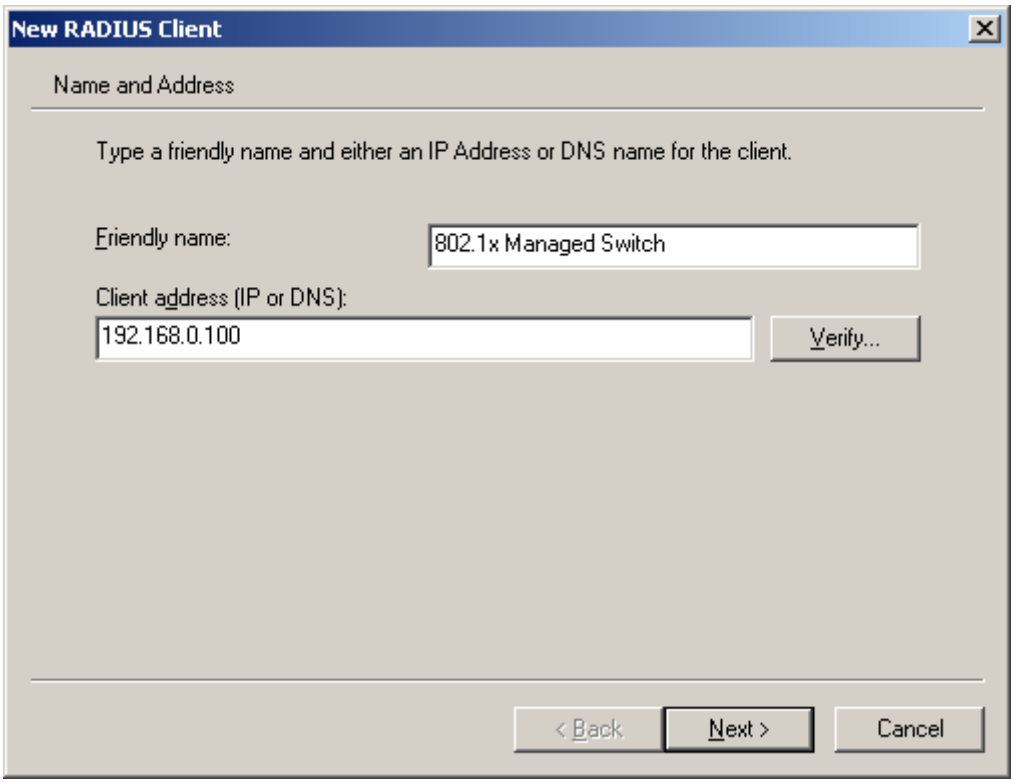


Figure 4-11-12: Windows Server RADIUS Server Setting

4. The shared **secret key** should be the same as the key configured on the **Industrial Managed Switch**.

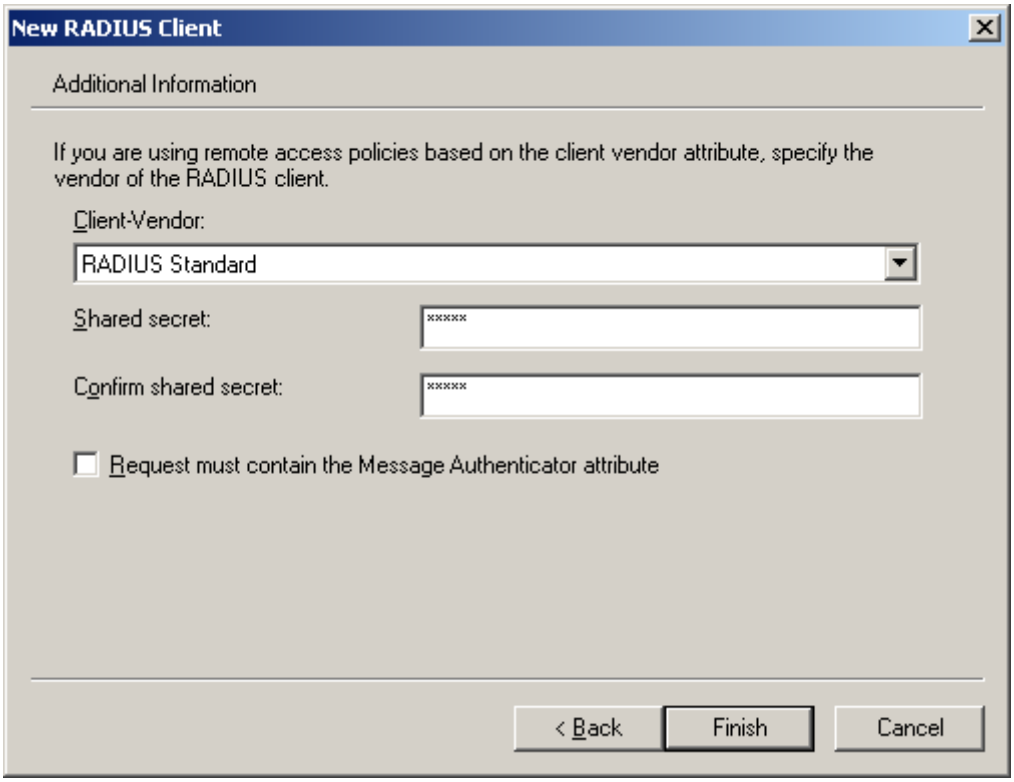


Figure 4-11-13: Windows Server RADIUS Server Setting

5. Configure ports attribute of 802.1X, the same as “802.1X Port Configuration”.

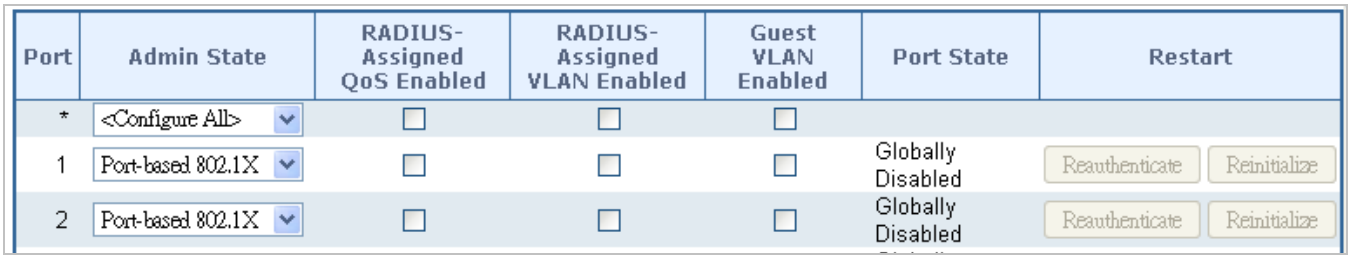


Figure 4-11-14: 802.1x Port Configuration

6. Create user data. The establishment of the user data needs to be created on the Radius Server PC. For example, the Radius Server founded on Win2003 Server, and then:

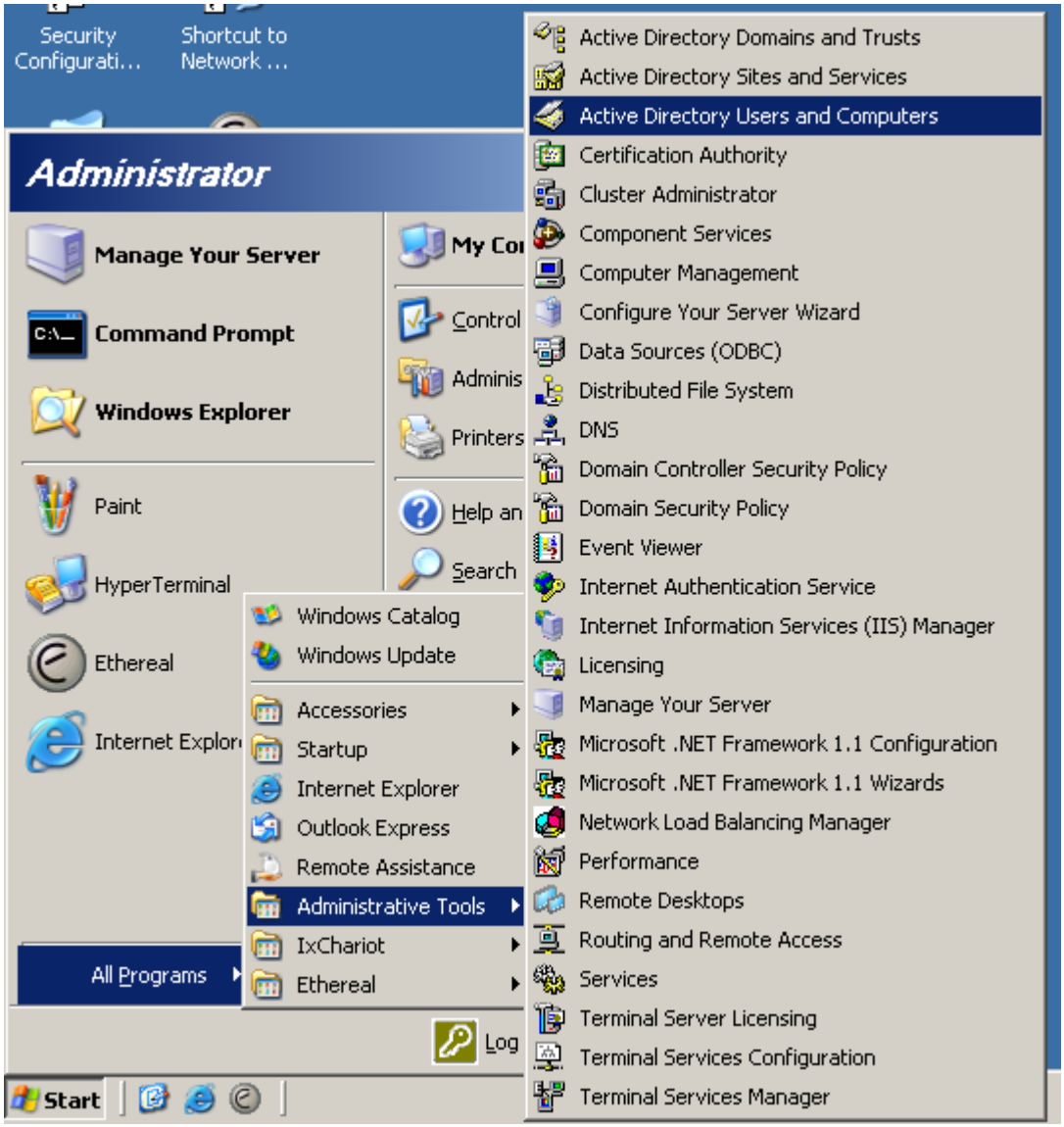


Figure 4-11-15: Windows 2003 AD Server Setting Path

7. Enter " **Active Directory Users and Computers**", create legal user data, the next, right-click a user what you created to enter properties, and what to be noticed:

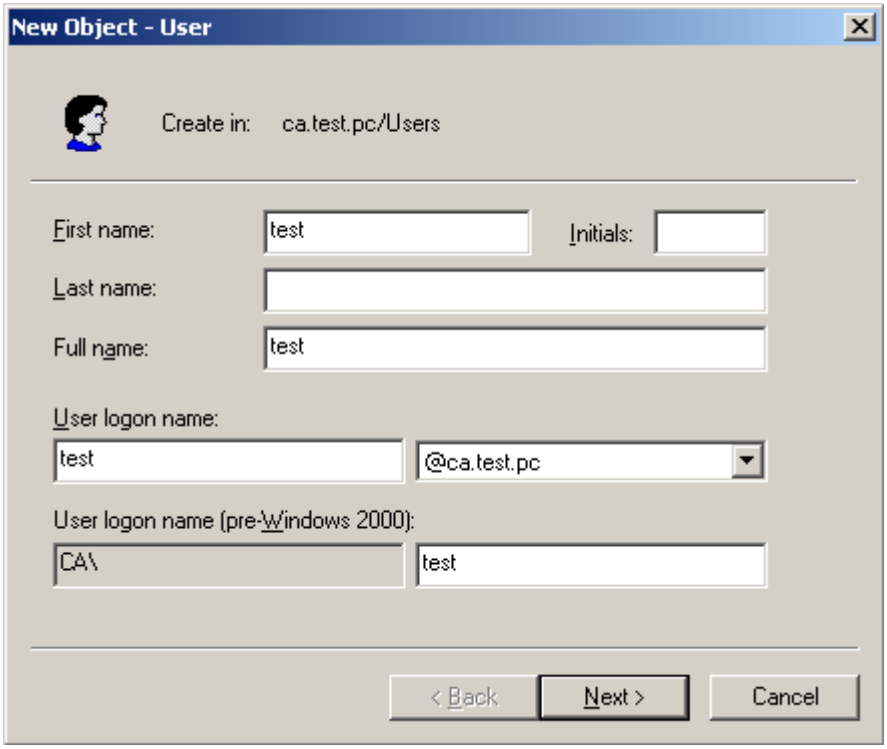


Figure 4-11-16: Add User Properties Screen

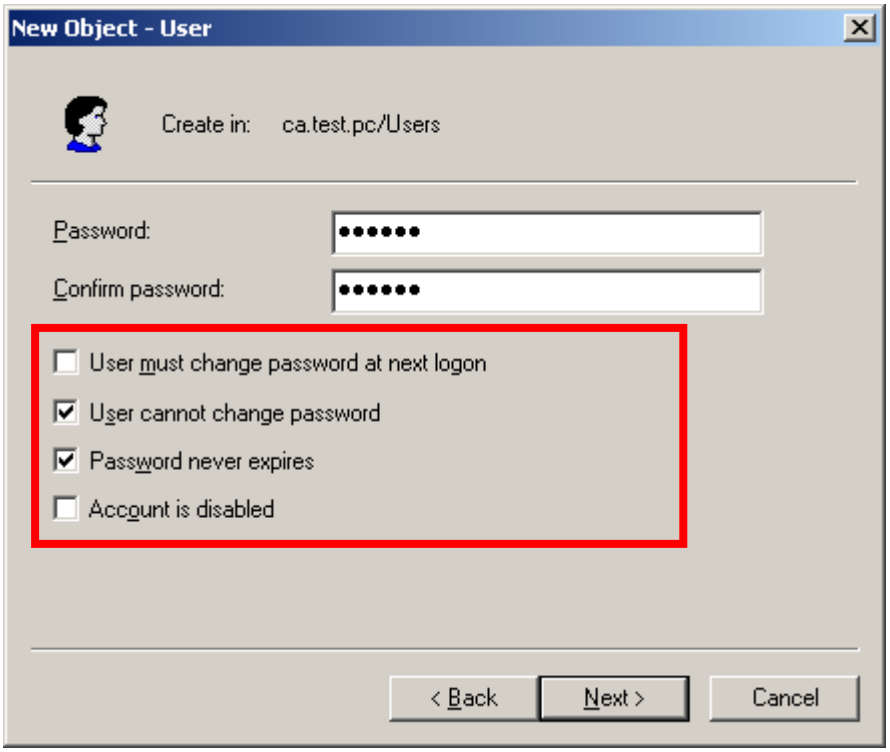


Figure 4-11-17: Add User Properties Screen

Note

Set the Ports Authenticate Status to "**Force Authorized**" if the port is connected to the RADIUS server or the port is an uplink port that is connected to another switch. Or once the 802.1X is set to work, the switch might not be able to access the RADIUS server.

4.11.10 802.1X Client Configuration

Windows XP is originally 802.1X support. As to other operating systems (windows 98SE, ME, 2000), an 802.1X client utility is needed. The following procedures show how to configure 802.1X Authentication in Windows XP.

Please note that if you want to change the 802.1x authentication type of a wireless client, i.e. switch to EAP-TLS from EAP-MD5, you must remove the current existing wireless network from your preferred connection first, and add it in again.

■ Configure Sample: EAP-MD5 Authentication

1. Go to **Start** > **Control Panel,** double-click on "**Network Connections**".
2. Right-click on the Local Network Connection.
3. Click "**Properties**" to open up the Properties setting window.

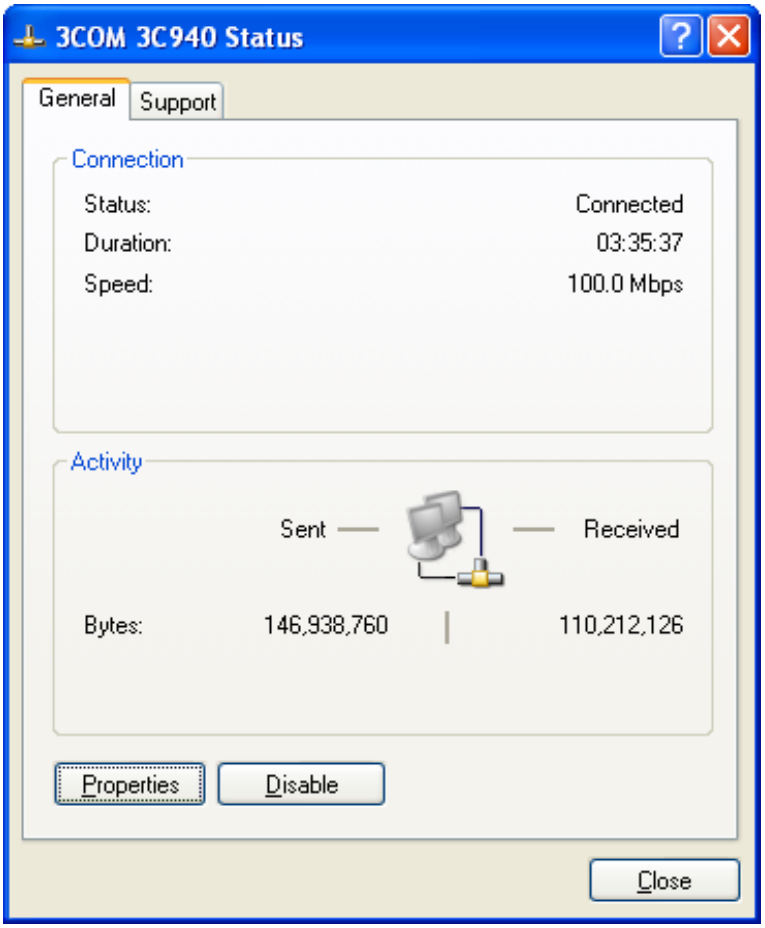


Figure 4-11-18

4. Select "**Authentication**" tab.

5. Select "**Enable network access control using IEEE 802.1X**" to enable 802.1x authentication.

6. Select "**MD-5 Challenge**" from the drop-down list box for EAP type.

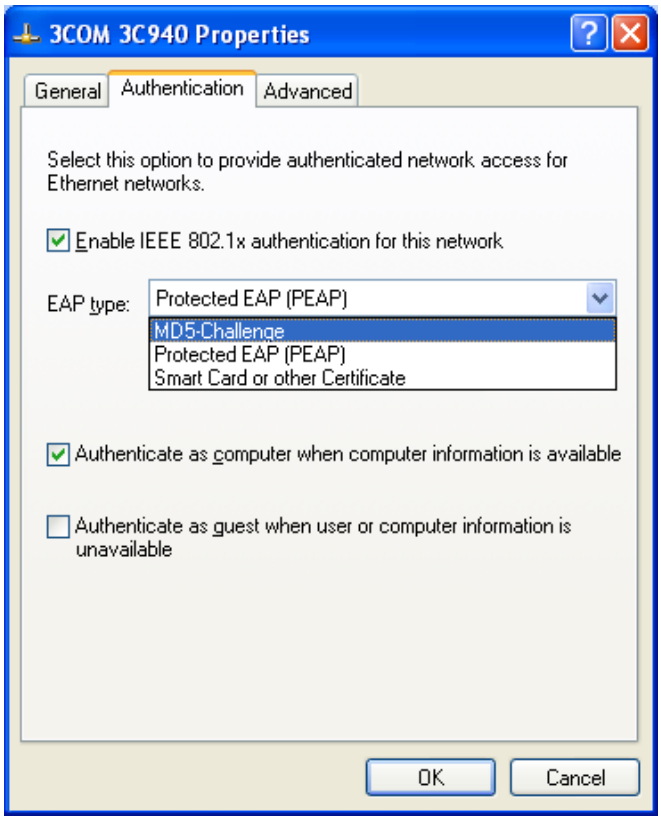


Figure 4-11-19

7. Click "**OK**".
8. When client has associated with the Managed Switch, a user authentication notice appears in system tray. Click on the notice to continue.

Figure 4-11-20: Windows Client Popup Login Request Message

9. Enter the user name, password and the logon domain that your account belongs.
10. Click "**OK**" to complete the validation process.

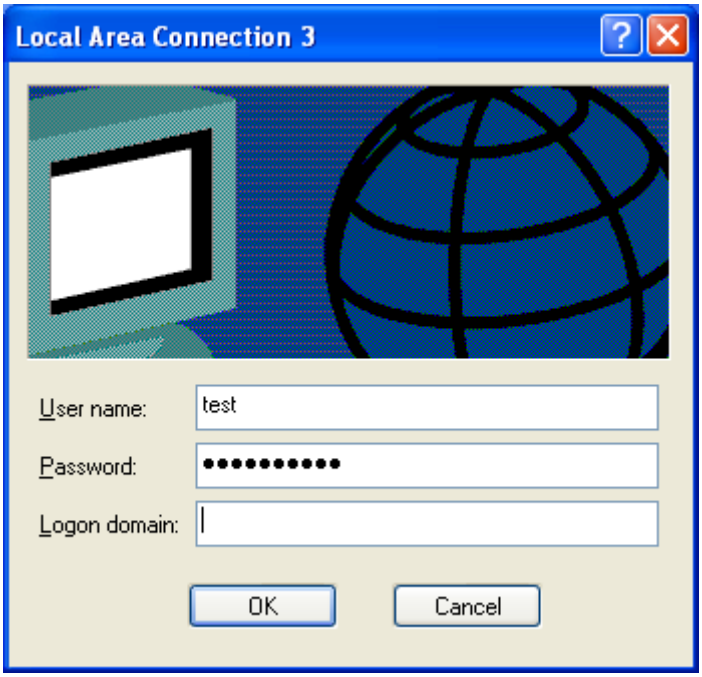


Figure 4-11-21

4.12 Security

This section is to control the access of the Industrial Managed Switch, including the user access and management control.

The Security page contains links to the following main topics:

- **Port Limit Control**
- **Access Management**
- **Access Management Statistics**
- **HTTPs**
- **SSH**
- **Port Security Status**
- **Port Security Detail**
- **DHCP Snooping**
- **DHCP Snooping Statistics**
- **IP Source Guard Configuration**
- **IP Source Guard Static Table**
- **ARP Inspection**
- **ARP Inspection Static Table**

4.12.1 Port Limit Control

This page allows you to configure the Port Security Limit Control system and port settings.

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module and Port Security module, which manages MAC addresses learnt on the port. The Limit Control configuration consists of two sections, a system and a port.

The Port Limit Control Configuration screen in Figure 4-12-1 appears.

Figure 4-12-1: Port Limit Control Configuration Overview Page Screenshot

The page includes the following fields:

System Configuration

Object	Description
• **Mode**	Indicates if Limit Control is globally enabled or disabled on the switch stack. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
• **Aging Enabled**	If checked, secured MAC addresses are subject to aging as discussed under Aging Period.
• **Aging Period**	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from

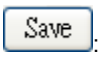
	the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

The table has one row for each port on the selected switch in the stack and a number of columns, which are:

Object	Description
• **Port**	The port number for which the configuration below applies.
• **Mode**	The Configuration All with available options will assign to whole ports. Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
• **Limit**	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The stack switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
• **Action**	The Configuration All with available options will assign to whole ports. If Limit is reached, the switch can take one of the following actions: **None**: Do not allow more than Limit MAC addresses on the port, but take no further action. **Trap**: If Limit + 1 MAC address is seen on the port send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded. **Shutdown**: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Boot the stack or elect a new master the switch, 2) Disable and re-enable Limit Control on the port or the stack switch, 3) Click the Reopen button. **Trap & Shutdown**: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.
• **State**	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: **Disabled**: Limit Control is either globally disabled or disabled on the port. **Ready**: The limit is not yet reached. This can be shown for all actions. **Limit Reached**: Indicates that the limit is reached on this port. This state can only be shown if Action is set to **None** or **Trap**. **Shutdown**: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to **Shut down** or **Trap & Shutdown**.
• **Reopen Button**	If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to **Shut down** in the Action section. Note, that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

Buttons



: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

4.12.2 Access Management

Configure access management table on this page. The maximum entry number is 16. If the application's type matches any one of the access management entries, it will allow access to the switch. The Access Management Configuration screen in Figure 4-12-2 appears.

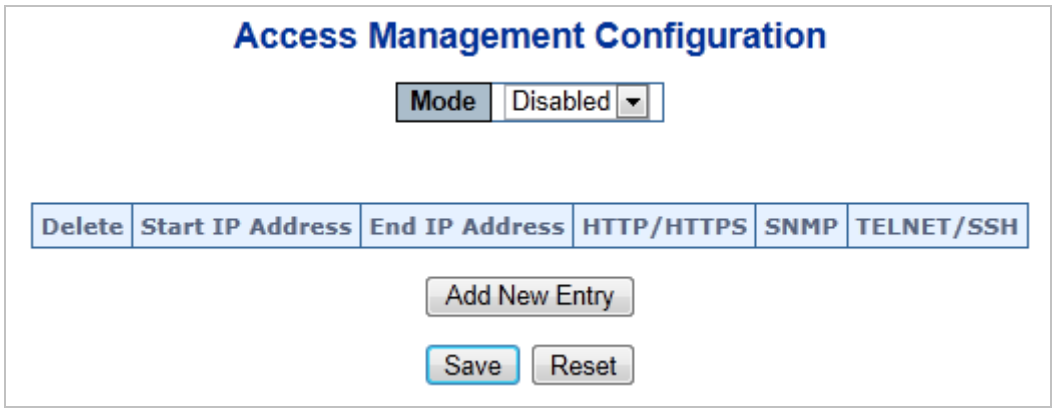


Figure 4-12-2: Access Management Configuration Overview Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the access management mode operation. Possible modes are: ■ **Enabled**: Enable access management mode operation. ■ **Disabled**: Disable access management mode operation.
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Start IP Address**	Indicates the start IP address for the access management entry.
• **End IP Address**	Indicates the end IP address for the access management entry.
• **HTTP/HTTPS**	Indicates the host can access the switch from HTTP/HTTPS interface that the host IP address matched the entry.
• **SNMP**	Indicates the host can access the switch from SNMP interface that the host IP address matched the entry.
• **TELNET/SSH**	Indicates the host can access the switch from TELNET/SSH interface that the host IP address matched the entry.

Buttons

Add New Entry: Click to add a new access management entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.12.3 Access Management Statistics

This page provides statistics for access management. The Access Management Statistics screen in Figure 4-12-3 appears.

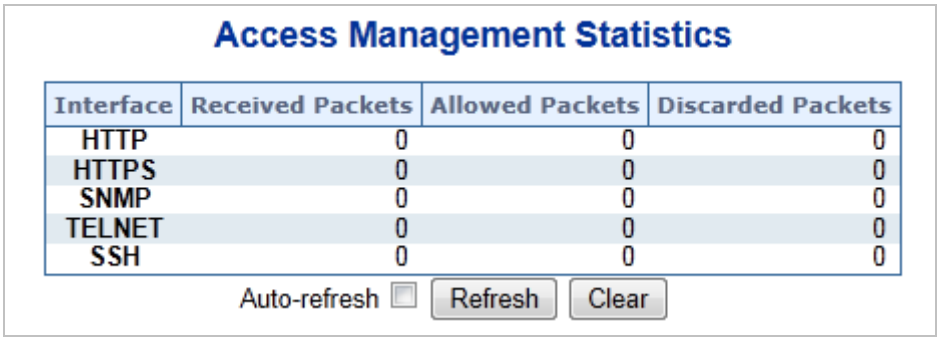


Figure 4-12-3: Access Management Statistics Overview Page Screenshot

The page includes the following fields:

Object	Description
• **Interface**	The interface that allowed remote host can access the **Industrial Managed Switch**.
• **Receive Packets**	The received packets number from the interface under access management mode is enabled.
• **Allowed Packets**	The allowed packets number from the interface under access management mode is enabled.
• **Discard Packets**	The discarded packets number from the interface under access management mode is enabled.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

4.12.4 HTTPs

Configure HTTPS on this page. The HTTPS Configuration screen in Figure 4-12-4 appears.

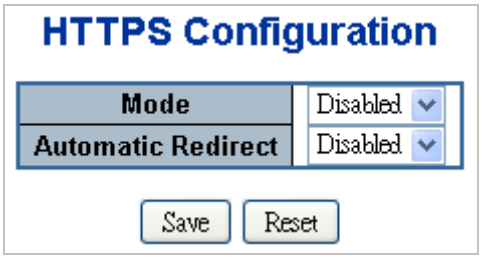


Figure 4-12-4: HTTPS Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the HTTPS mode operation. Possible modes are: ■ **Enabled**: Enable HTTPS mode operation. ■ **Disabled**: Disable HTTPS mode operation.
• **Automatic Redirect**	Indicates the HTTPS redirect mode operation. Automatic redirect web browser to HTTPS during HTTPS mode enabled. Possible modes are: ■ **Enabled**: Enable HTTPS redirect mode operation. ■ **Disabled**: Disable HTTPS redirect mode operation.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.12.5 SSH

Configure SSH on this page. This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status. The SSH Configuration screen in Figure 4-12-5 appears.

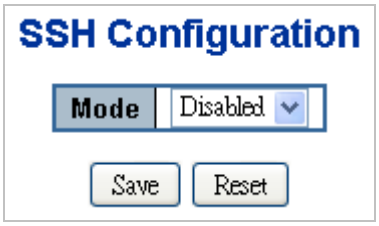


Figure 4-12-5: SSH Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Indicates the SSH mode operation. Possible modes are: **Enabled**: Enable SSH mode operation. **Disabled**: Disable SSH mode operation.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.12.6 Port Security Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly

from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and the other with the actual port status. The Port Security Status screen in Figure 4-12-6 appears.

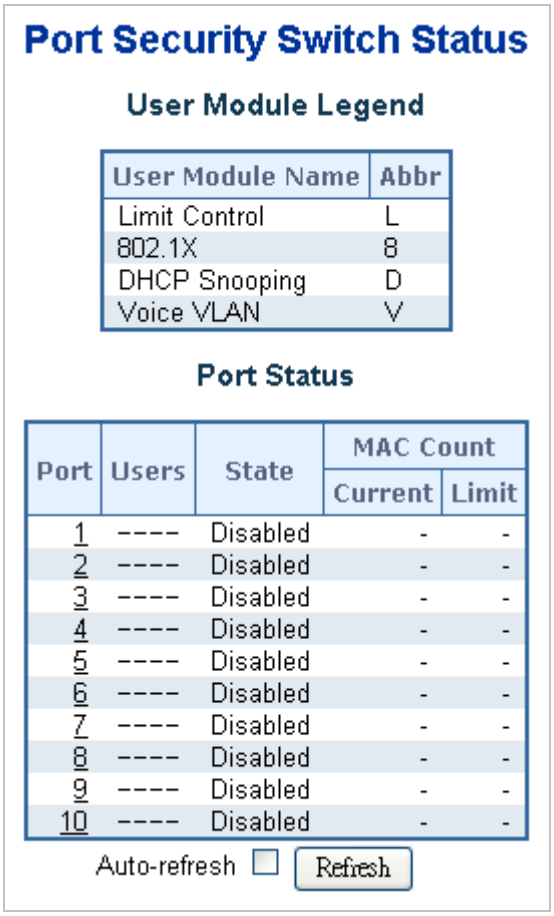


Figure 4-12-6: Port Security Status Screen Page Screenshot

The page includes the following fields:

User Module Legend

The legend shows all user modules that may request Port Security services.

Object	Description
• **User Module Name**	The full name of a module that may request Port Security services.
• **Abbr**	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status

The table has one row for each port on the selected switch in the switch and a number of columns, which are:

Object	Description
• **Port**	The port number for which the status applies. Click the port number to see the status for this particular port.
• **Users**	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.
• **State**	Shows the current state of the port. It can take one of four values: **Disabled**: No user modules are currently using the Port Security service. **Ready**: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. **Limit Reached**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. **Shutdown**: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.
• **MAC Count (Current, Limit)**	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.12.7 Port Security Detail

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The Port Security Detail screen in Figure 4-12-7 appears.

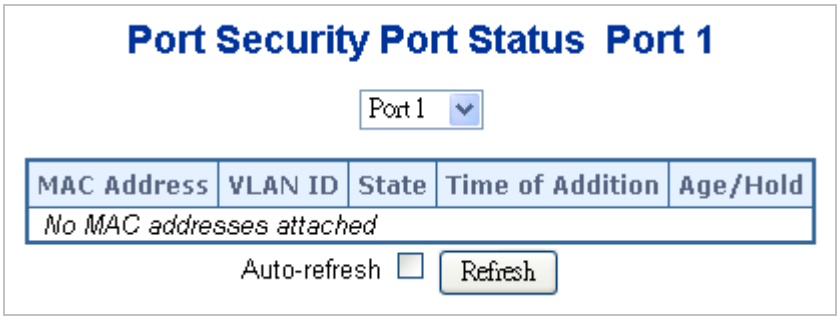


Figure 4-12-7: Port Security Detail Screen Page Screenshot

The page includes the following fields:

Object	Description
• **MAC Address & VLAN ID**	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
• **State**	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
• **Time of Addition**	Shows the date and time when this MAC address was first seen on the port.
• **Age/Hold**	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.12.8 DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of DUT when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server. Configure DHCP Snooping on this page. The DHCP Snooping Configuration screen in Figure 4-12-8 appears.

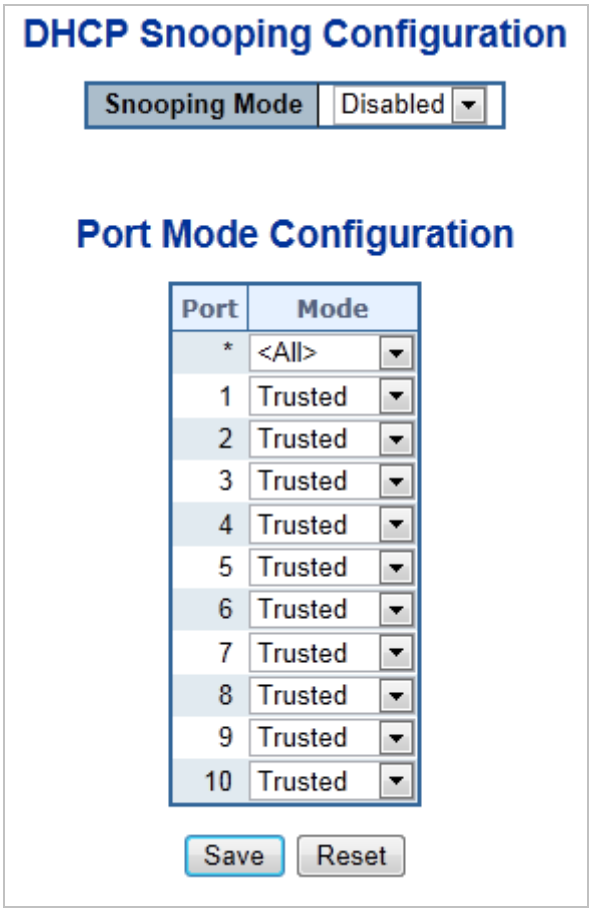


Figure 4-12-8: DHCP Snooping Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Snooping Mode**	Indicates the DHCP snooping mode operation. Possible modes are: **Enabled**: Enable DHCP snooping mode operation. When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports. **Disabled**: Disable DHCP snooping mode operation.
• **Port Mode**	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted sources of the DHCP message. **Untrusted**: Configures the port as untrusted sources of the DHCP message. **All** means all ports will have one specific setting

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.12.9 DHCP Snooping Statistics

This page provides statistics for DHCP snooping. The statistics only counter packet under DHCP snooping mode is enabled and relay mode is disabled. And it doesn't count the DHCP packets for system DHCP client. The DHCP Snooping Port Statistics screen in Figure 4-12-9 appears.

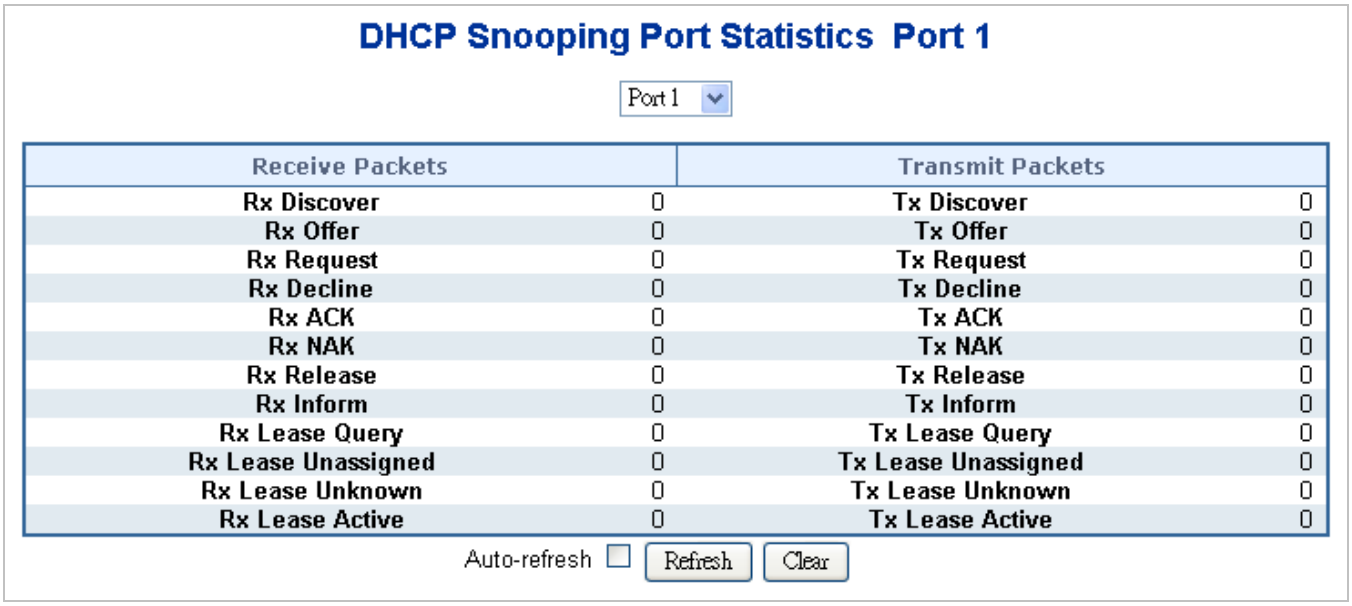


Figure 4-12-9: DHCP Snooping Port Statistics Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Rx and Tx Discover**	The number of discover (option 53 with value 1) packets received and transmitted.
• **Rx and Tx Offer**	The number of offer (option 53 with value 2) packets received and transmitted.
• **Rx and Tx Request**	The number of request (option 53 with value 3) packets received and transmitted.
• **Rx and Tx Decline**	The number of decline (option 53 with value 4) packets received and transmitted.
• **Rx and Tx ACK**	The number of ACK (option 53 with value 5) packets received and transmitted.
• **Rx and Tx NAK**	The number of NAK (option 53 with value 6) packets received and transmitted.
• **Rx and Tx Release**	The number of release (option 53 with value 7) packets received and transmitted.
• **Rx and Tx Inform**	The number of inform (option 53 with value 8) packets received and transmitted.

• **Rx and Tx Lease Query**	The number of lease query (option 53 with value 10) packets received and transmitted.
• **Rx and Tx Lease Unassigned**	The number of lease unassigned (option 53 with value 11) packets received and transmitted.
• **Rx and Tx Lease Unknown**	The number of lease unknown (option 53 with value 12) packets received and transmitted.
• **Rx and Tx Lease Active**	The number of lease active (option 53 with value 13) packets received and transmitted.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

4.12.10 IP Source Guard Configuration

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. This page provides IP Source Guard related configuration. The IP Source Guard Configuration screen in Figure 4-12-10 appears.

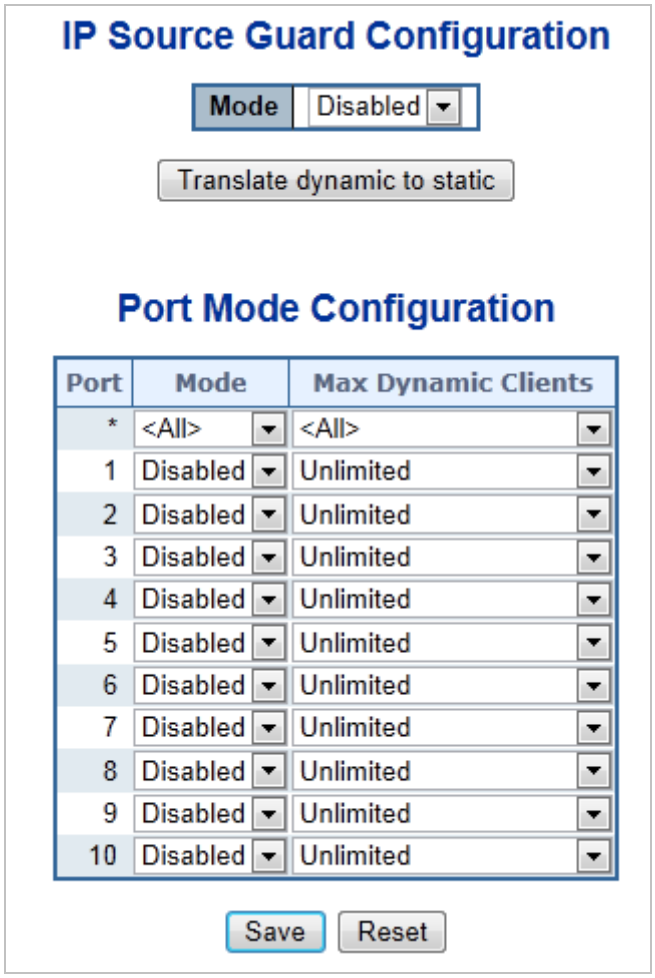


Figure 4-12-10: IP Source Guard Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode of IP Source Guard Configuration**	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
• **Port Mode Configuration**	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port. **All** means all ports will have one specific setting.
• **Max Dynamic Clients**	Specify the maximum number of dynamic clients can be learned on given ports. This value can be 0, 1, 2 and unlimited. If the port mode is enabled and the value of max dynamic client is equal 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port. **All** means all ports will have one specific setting.

Buttons

Translate dynamic to static : Click to translate all dynamic entries to static entries.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.12.11 IP Source Guard Static Table

This page provides Static IP Source Guard Table. The Static IP Source Guard Table screen in Figure 4-12-11 appears.

Figure 4-12-11: Static IP Source Guard Table Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **VLAN ID**	The VLAN ID for the settings.
• **IP Address**	Allowed Source IP address.
• **MAC address**	Allowed Source MAC address.

Buttons

Add New Entry: Click to add a new entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.12.12 ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT. This page provides ARP Inspection related configuration. The ARP Inspection Configuration screen in Figure 4-12-12 appears.

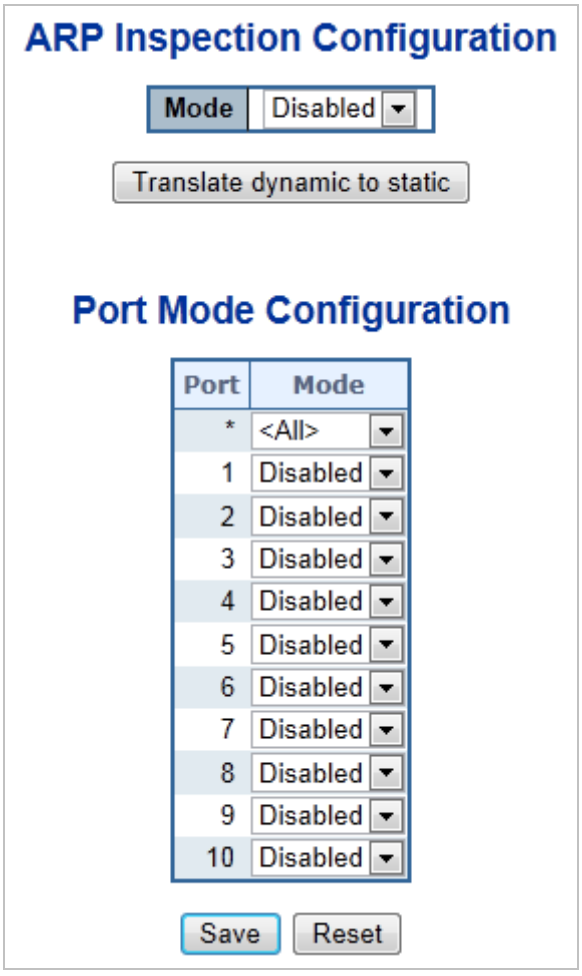


Figure 4-12-12: ARP Inspection Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Mode of ARP Inspection Configuration**	Enable the Global ARP Inspection or disable the Global ARP Inspection.
• **Port Mode Configuration**	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. **All** means all ports will have one specific setting.

Buttons

Translate dynamic to static : Click to translate all dynamic entries to static entries.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.12.13 ARP Inspection Static Table

This page provides Static ARP Inspection Table. The Static ARP Inspection Table screen in Figure 4-12-13 appears.

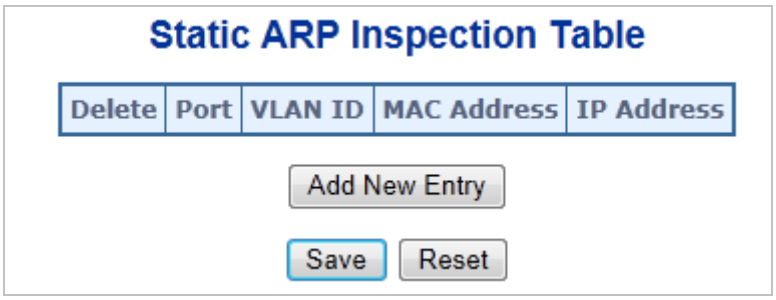


Figure 4-12-13: Static ARP Inspection Table Screen Page Screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **Port**	The logical port for the settings.
• **VLAN ID**	The VLAN ID for the settings.
• **MAC Address**	Allowed Source MAC address in ARP request packets.
• **IP Address**	Allowed Source IP address in ARP request packets.

Buttons

Add New Entry: Click to add a new entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.13 MAC Address Table

Switching of frames is based upon the DMAC address contained in the frame. The Managed Switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

4.13.1 MAC Address Table Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here. The MAC Address Table Configuration screen in Figure 4-13-1 appears.

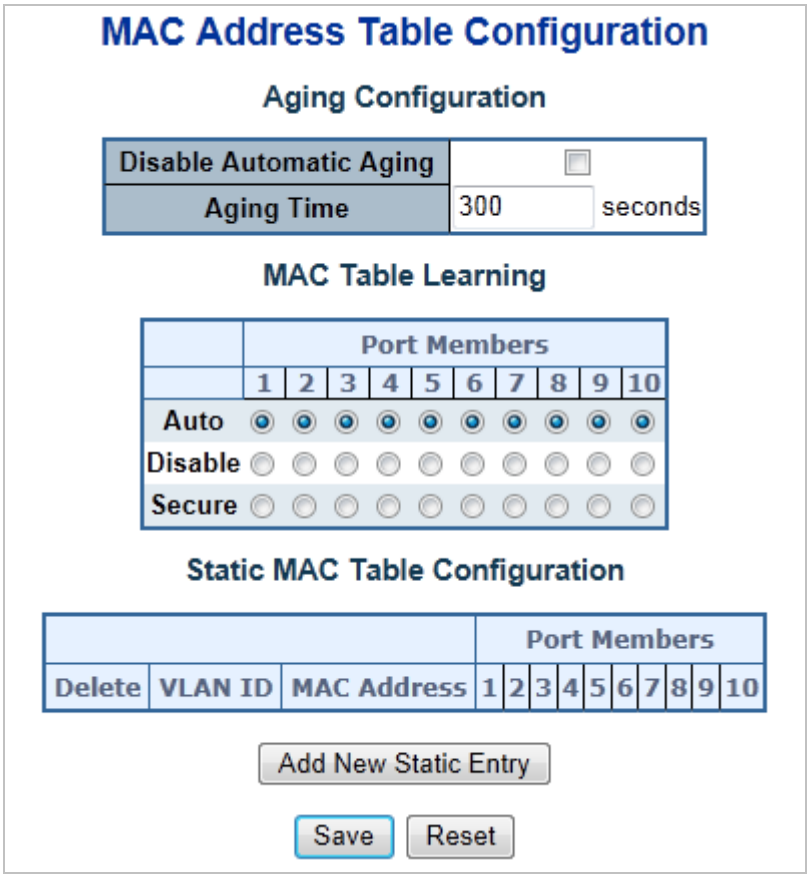


Figure 4-13-1: MAC Address Table Configuration Page Screenshot

The page includes the following fields:

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Object	Description
• **Disable Automatic Aging**	Enables/disables the automatic aging of dynamic entries
• **Aging Time**	The time after which a learned entry is discarded. By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging. (Range: 10-10000000 seconds; Default: 300 seconds)

MAC Table Learning

If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Object	Description
• **Auto**	Learning is done automatically as soon as a frame with unknown SMAC is received.
• **Disable**	No learning is done.
• **Secure**	Only static MAC entries are learned, all other frames are dropped. **Note:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **VLAN ID**	The VLAN ID of the entry.
• **MAC Address**	The MAC address of the entry.
• **Port Members**	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Buttons

Add New Static Entry: Click to add a new entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.13.2 MAC Address Table Status

Dynamic MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to **8192** entries, and is sorted first by VLAN ID, then by MAC address. The MAC Address Table screen in Figure 4-13-2 appears.

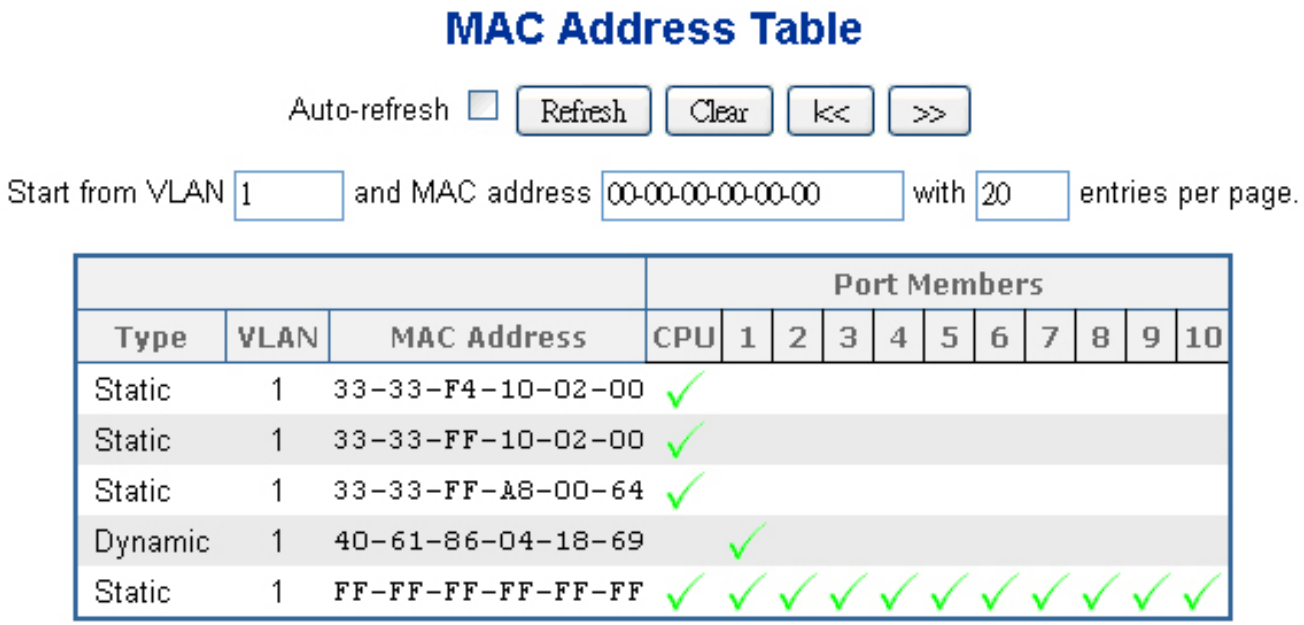

MAC Address Table
Auto-refresh
Refresh
Clear
<<
>>
Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.
Port Members
Type VLAN MAC Address CPU 1 2 3 4 5 6 7 8 9 10
Static 1 33-33-F4-10-02-00
Static 1 33-33-FF-10-02-00
Static 1 33-33-FF-A8-00-64
Dynamic 1 40-61-86-04-18-69
Static 1 FF-FF-FF-FF-FF-FF

Figure 4-13-2: MAC Address Table Status Page Screenshot

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "**entries per page"** input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "**Start from MAC address**" and "**VLAN**" input fields allow the user to select the starting point in the MAC Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next MAC Table match.

In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The "**>>**" will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table. Use the "**|<<**" button to start over.

The page includes the following fields:

Object	Description
• **Type**	Indicates whether the entry is a static or dynamic entry.
• **VLAN**	The VLAN ID of the entry.
• **MAC Address**	The MAC address of the entry.
• **Port Members**	The ports that are members of the entry.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Clear: Flushes all dynamic entries.

<<: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.13.3 Dynamic ARP Inspection Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. The Dynamic ARP Inspection Table screen in Figure 4-13-3 appears.

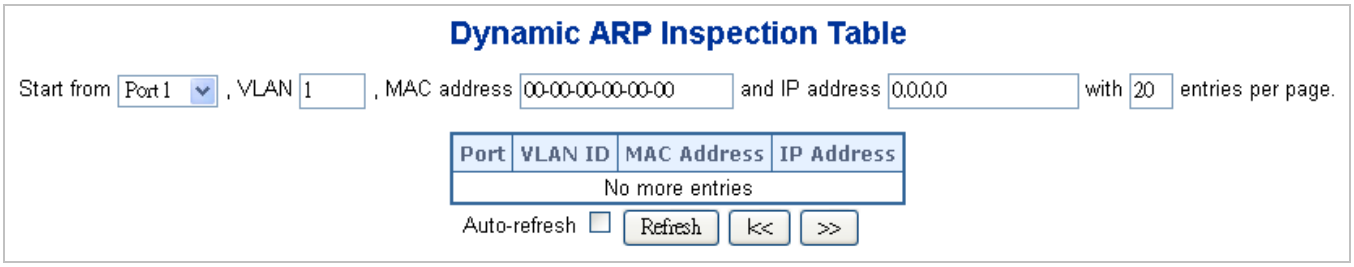


Figure 4-13-3: Dynamic ARP Inspection Table Screenshot

Navigating the ARP Inspection Table

Each page shows up to 999 entries from the Dynamic ARP Inspection table, default being 20, selected through the "**entries per page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "**Start from port address**", "**VLAN**", "**MAC address**" and "**IP address**" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “**>>**” will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “**|<<**” button to start over.

The page includes the following fields:

Object	Description
• **Port**	Switch Port Number for which the entries are displayed.
• **VLAN ID**	VLAN-ID in which the ARP traffic is permitted.
• **MAC Address**	User MAC address of the entry.
• **IP Address**	User IP address of the entry.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: : Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.13.4 Dynamic IP Source Guard Table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address. The Dynamic IP Source Guard Table screen in Figure 4-13-4 appears.

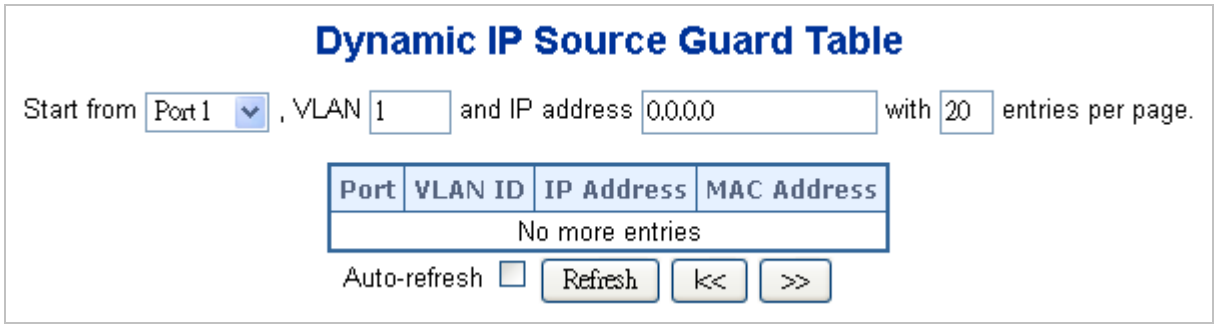


Figure 4-13-4: Dynamic IP Source Guard Table Screenshot

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "**entries per page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table. The "**Start from port address**", "**VLAN**", "**IP address**" and "**IP mask**" input fields allow the user to select the

starting point in the Dynamic IP Source Guard Table. Clicking the "**Refresh**" button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a "**Refresh**" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The "**>>**" will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the "**|<<**" button to start over.

The page includes the following fields:

Object	Description
• **Port**	Switch Port Number for which the entries are displayed.
• **VLAN ID**	VLAN-ID in which the IP traffic is permitted.
• **IP Address**	User IP Address of the entry.
• **MAC Address**	Source MAC Address.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

|<<: Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.14 LLDP

4.14.1 Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in **Type Length Value (TLV)** format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

4.14.2 LLDP Configuration

This page allows the user to inspect and configure the current LLDP port settings. The LLDP Configuration screen in Figure 4-14-1 appears.

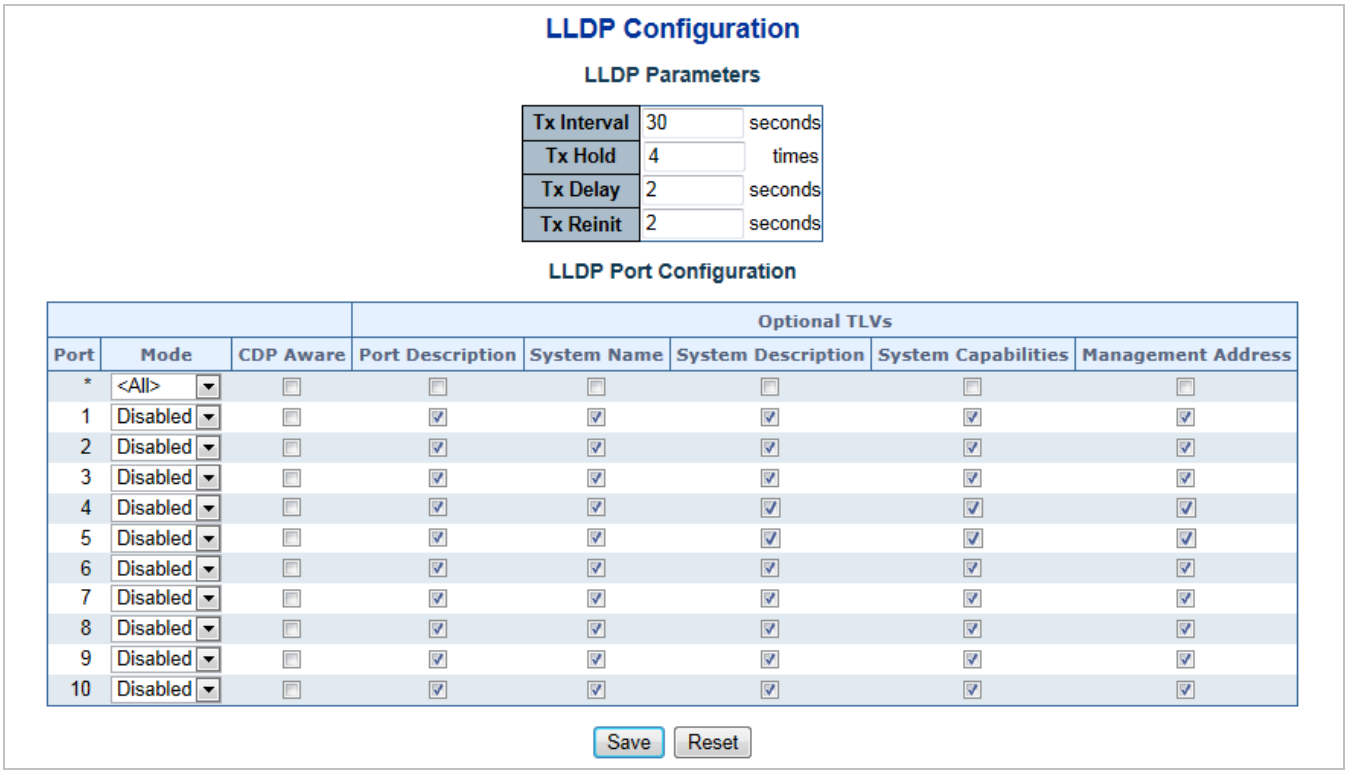


Figure 4-14-1: LLDP Configuration Page Screenshot

The page includes the following fields:

LLDP Parameters

Object	Description
• **Tx Interval**	The switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds. Default: **30** seconds This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)
• **Tx Hold**	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times. TTL in seconds is based on the following rule: (Transmission Interval * Hold time Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
• **Tx Delay**	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
• **Tx Reinit**	When a port is disabled, LLDP is disabled or the switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

Object	Description
• **Port**	The switch port number of the logical LLDP port.
• **Mode**	Select LLDP mode. **All** means all ports will have one specific setting. ■ **Rx only** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. ■ **Tx only** The switch will drop LLDP information received from neighbors, but will send out LLDP information. ■ **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbors. ■ **Enabled** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
• **CDP Aware**	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbor's table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbor's table as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbor's table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

	Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbor's table. If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.
• **Port Description**	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
• **System Name**	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
• **System Description**	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
• **System Capabilities**	Optional TLV: When checked the "system capability" is included in LLDP information transmitted. The system capabilities identify the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.
• **Management Address**	Optional TLV: When checked the "management address" is included in LLDP information transmitted. The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.14.3 LLDP-MED Configuration

This page allows you to configure the LLDP-MED. The LLDP-MED Configuration screen in Figure 4-14-2 appears.

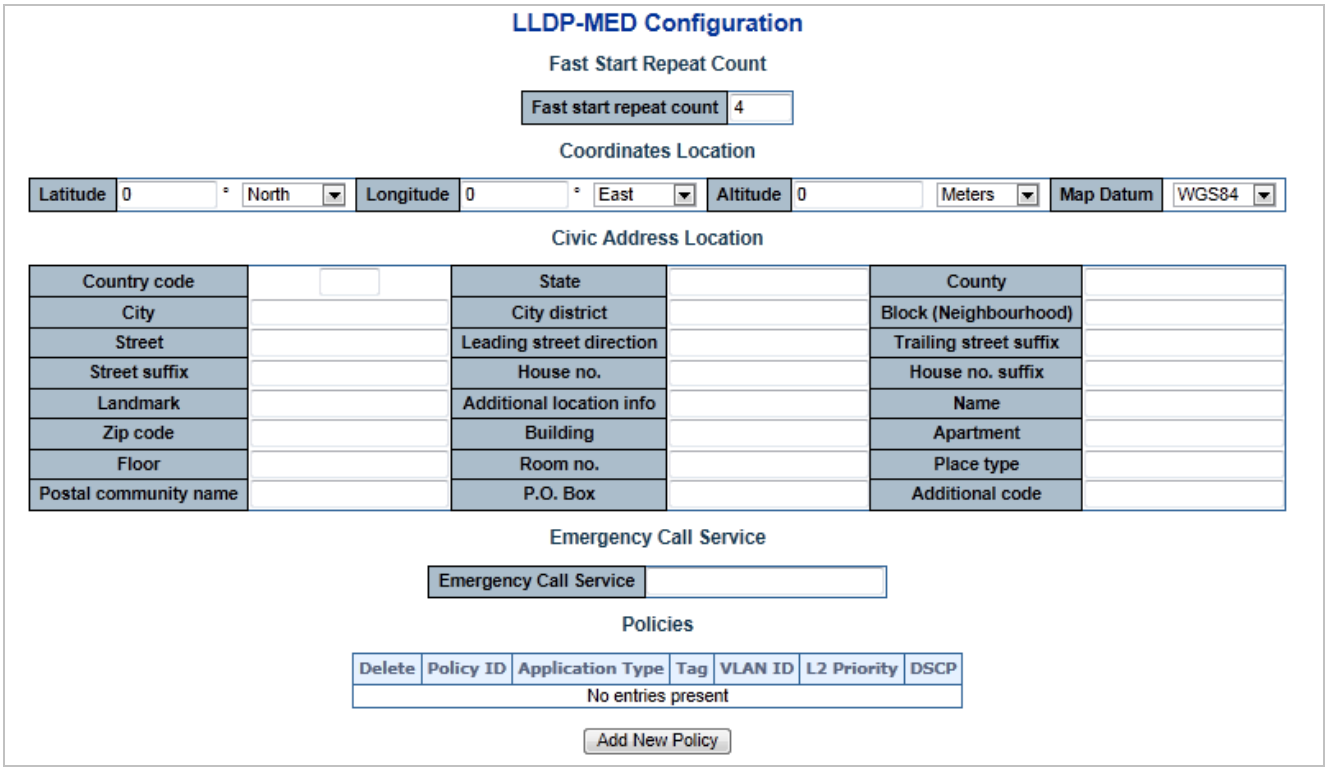


Figure 4-14-2: LLDP-MED Configuration Page Screenshot

The page includes the following fields:

Fast Start Repeat Count

Object	Description
• **Fast start repeat count**	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors. Because there is a risk that a LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility for that the neighbors has received the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

Coordinates Location

Object	Description
• **Latitude**	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.
• **Longitude**	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.
• **Altitude**	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). ■ **Meters**: Representing meters of Altitude defined by the vertical datum specified. ■ **Floors**: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
• **Map Datum**	The Map Datum used for the coordinates given in this Option ■ **WGS84**: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, and Prime Meridian Name: Greenwich. ■ **NAD83/NAVD88**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; the associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). ■ **NAD83/MLLW**: North American Datum 1983, CRS Code 4269, Prime

	Meridian Name: Greenwich; the associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Object	Description
• **Country code**	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
• **State**	National subdivisions (state, canton, region, province, prefecture).
• **County**	County, parish, gun (Japan), district.
• **City**	City, township, shi (Japan) - Example: Copenhagen
• **City district**	City division, borough, city district, ward, chou (Japan)
• **Block (Neighborhood)**	Neighborhood, block
• **Street**	Street - Example: Poppelvej
• **Leading street direction**	Leading street direction - Example: N
• **Trailing street suffix**	Trailing street suffix - Example: SW
• **Street suffix**	Street suffix - Example: Ave, Platz
• **House no.**	House number - Example: 21
• **House no. suffix**	House number suffix - Example: A, 1/2
• **Landmark**	Landmark or vanity address - Example: Columbia University
• **Additional location info**	Additional location info - Example: South Wing
• **Name**	Name (residence and office occupant) - Example: Flemming John
• **Zip code**	Postal/zip code - Example: 2791
• **Building**	Building (structure) - Example: Low Library
• **Apartment**	Unit (Apartment, suite) - Example: Apt 42
• **Floor**	Floor - Example: 4
• **Room no.**	Room number - Example: 450F
• **Place type**	Place type - Example: Office
• **Postal community name**	Postal community name - Example: Leonia
• **P.O. Box**	Post office box (P.O. BOX) - Example: 12345
• **Additional code**	Additional code - Example: 1320300003

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Object	Description
• **Emergency Call Service**	Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Object	Description
• **Delete**	Check to delete the policy. It will be deleted during the next save.

• **Policy ID**	ID for the policy. This is auto generated and shall be used when selecting the polices that shall be mapped to the specific ports.
• **Application Type**	Intended use of the application types: **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **Voice Signaling (conditional)** - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. **Guest Voice Signaling (conditional)** - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. **Video Conferencing** **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. **Video Signaling (conditional)** - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
• **Tag**	Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. **Untagged** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. **Tagged** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
• **VLAN ID**	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003
• **L2 Priority**	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
• **DSCP**	DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Port Policies Configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.

Object	Description

• **Port**	The port number for which the configuration applies.
• **Policy ID**	The set of policies that shall apply for a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies

Buttons

Add New Policy: click to add new policy.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.14.4 LLDP-MED Neighbor

This page provides a status overview for all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP-MED Neighbor Information screen in Figure 4-14-3 appears. The columns hold the following information:

Figure 4-14-3: LLDP-MED Neighbor Information with no LLDP-MED device detected

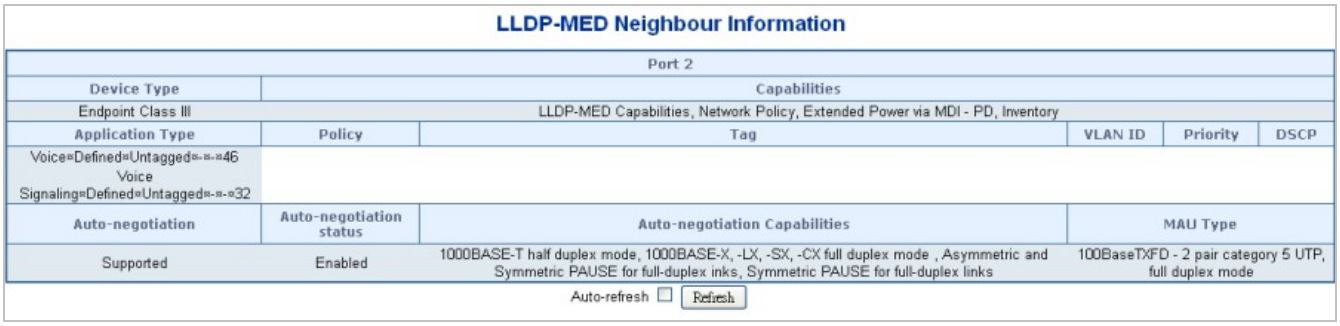


Figure 4-14-4: LLDP-MED Neighbor Information with LLDP-MED device detected

The page includes the following fields:

Fast Start Repeat Count

Object	Description
• **Port**	The port on which the LLDP frame was received.
• **Device Type**	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. **LLDP-MED Endpoint Device Definition** Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. Fore-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

	LLDP-MED Generic Endpoint (Class I) The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management. **LLDP-MED Media Endpoint (Class II)** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery. **LLDP-MED Communication Endpoint (Class III)** The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management
• **LLDP-MED Capabilities**	LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved
• **Application Type**	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. **Voice Signaling** - for use in network topologies that require a different policy for the voice signaling than for the voice media. **Guest Voice** - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. Guest Voice Signaling - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. **Streaming Video** - for use by broadcast or multicast based video content

	distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. **Video Signaling** - for use in network topologies that require a separate policy for the video signaling than for the video media.
• **Policy**	Policy **Unknown**: The network policy for the specified application type is currently unknown. **Defined**: The network policy is defined.
• **TAG**	TAG is indicating whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged **Untagged**: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. **Tagged**: The device is using the IEEE 802.1Q tagged frame format
• **VLAN ID**	VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
• **Priority**	Priority is the Layer 2 priority to be used for the specified application type. One of eight priority levels (0 through 7)
• **DSCP**	DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
• **Auto-negotiation**	**Auto-negotiation** identifies if MAC/PHY auto-negotiation is supported by the link partner.
• **Auto-negotiation status**	**Auto-negotiation status** identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
• **Auto-negotiation Capabilities**	**Auto-negotiation Capabilities** shows the link partners MAC/PHY capabilities.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.14.5 Neighbor

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Neighbor Information screen in Figure 4-14-4 appears.

Figure 4-14-4: LLDP Neighbor Information Page Screenshot

The page includes the following fields:

Object	Description
• **Local Port**	The port on which the LLDP frame was received.
• **Chassis ID**	The Chassis ID is the identification of the neighbor's LLDP frames.
• **Remote Port ID**	The Remote Port ID is the identification of the neighbor port.
• **System Name**	System Name is the name advertised by the neighbor unit.
• **Port Description**	Port Description is the port description advertised by the neighbor unit.
• **System Capabilities**	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
• **Management Address**	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.14.6 Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch. The LLDP Statistics screen in Figure 4-14-5 appears.

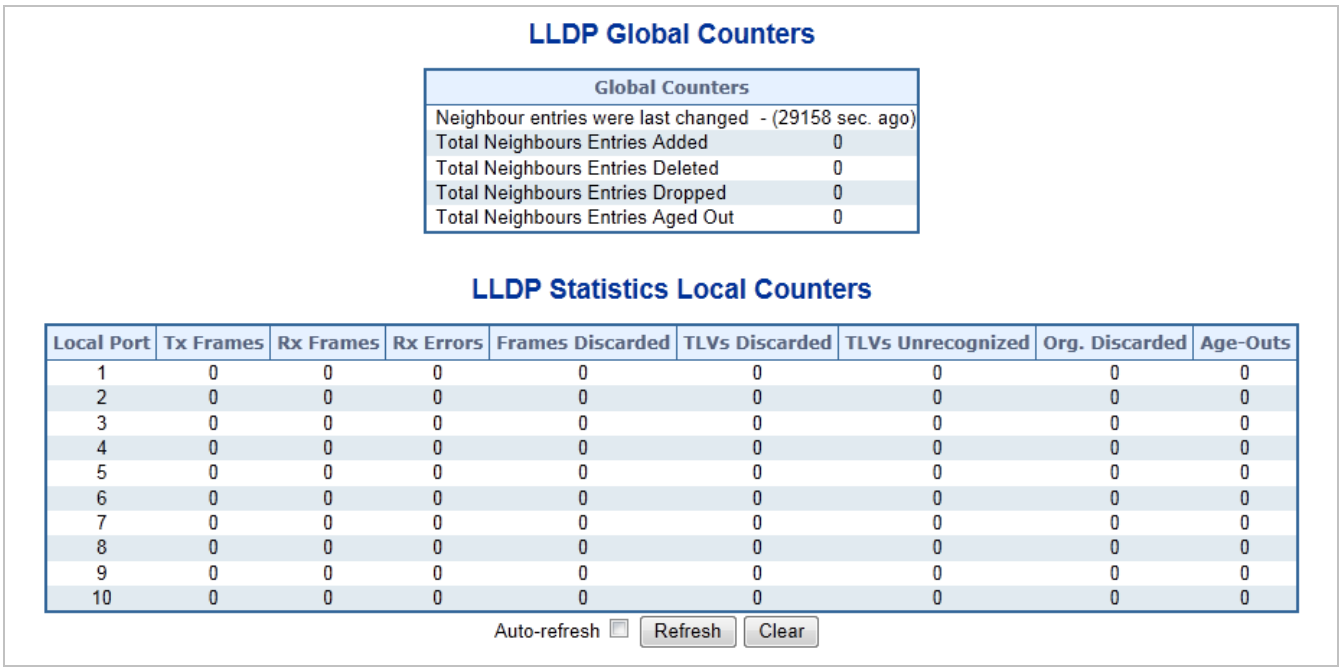

LLDP Global Counters
Global Counters
Neighbour entries were last changed - (29158 sec. ago)
Total Neighbours Entries Added 0
Total Neighbours Entries Deleted 0
Total Neighbours Entries Dropped 0
Total Neighbours Entries Aged Out 0
LLDP Statistics Local Counters
Local Port | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs
1 0 0 0 0 0 0 0 0
2 0 0 0 0 0 0 0 0
3 0 0 0 0 0 0 0 0
4 0 0 0 0 0 0 0 0
5 0 0 0 0 0 0 0 0
6 0 0 0 0 0 0 0 0
7 0 0 0 0 0 0 0 0
8 0 0 0 0 0 0 0 0
9 0 0 0 0 0 0 0 0
10 0 0 0 0 0 0 0 0
Auto-refresh
Refresh
Clear

Figure 4-14-5: LLDP Statistics Page Screenshot

The page includes the following fields:

Global Counters

Object	Description
• **Neighbor entries were last changed at**	It also shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
• **Total Neighbors Entries Added**	Shows the number of new entries added since switch reboot.
• **Total Neighbors Entries Deleted**	Shows the number of new entries deleted since switch reboot.
• **Total Neighbors Entries Dropped**	Shows the number of LLDP frames dropped due to that the entry table was full.
• **Total Neighbors Entries Aged Out**	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Object	Description
• **Local Port**	The port on which LLDP frames are received or transmitted.
• **Tx Frames**	The number of LLDP frames transmitted on the port.
• **Rx Frames**	The number of LLDP frames received on the port.
• **Rx Errors**	The number of received LLDP frames containing some kind of error.
• **Frames Discarded**	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
• **TLVs Discarded**	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
• **TLVs Unrecognized**	The number of well-formed TLVs, but with an unknown type value.
• **Org. Discarded**	The number of organizationally TLVs received.
• **Age-Outs**	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the local counters. All counters (including global counters) are cleared upon reboot.

4.15 Diagnostics

This section provide the Physical layer and IP layer network diagnostics tools for troubleshoot. The diagnostic tools are designed for network manager to help them quickly diagnose problems between point to point and better service customers.

Use the Diagnostics menu items to display and configure basic administrative details of the Managed Switch. Under System the following topics are provided to configure and view the system information:
This section has the following items:

- **Ping**
- **IPv6 Ping**
- **Remote IP Ping**
- **Cable Diagnostics**

PING

The ping and IPv6 ping allow you to issue ICMP PING packets to troubleshoot IP connectivity issues. The Managed Switch transmits ICMP packets, and the sequence number and roundtrip time are displayed upon reception of a reply.

Cable Diagnostics

The Cable Diagnostics is performing tests on copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling. There might be two statuses as follow:

- If the link is established on the twisted-pair interface in 1000Base-T mode, the Cable Diagnostics can run without disruption of the link or of any data transfer.
- If the link is established in 100Base-TX or 10Base-T, the Cable Diagnostics cause the link to drop while the diagnostics are running.

After the diagnostics are finished, the link is reestablished. And the following functions are available.

- Coupling between cable pairs.
- Cable pair termination
- Cable Length

4.15.1 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press "**Start**", 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-15-1 appears.

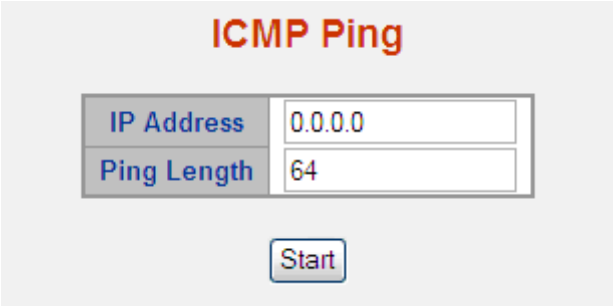


Figure 4-15-1: ICMP Ping Page Screenshot

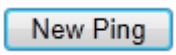
The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address.
• **Ping Length**	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
• **Ping Count**	The count of the ICMP packet. Values range from 1 time to 60 times.
• **Ping Interval**	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Be sure the target IP Address is within the same network subnet of the switch, or you had setup the correct gateway IP address.

Button

: Click to start transmitting ICMP packets.



: Click to re-start diagnostics with PING.

4.15.2 IPv6 Ping

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press "**Start**", 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMPv6 Ping screen in Figure 4-15-2 appears.

Figure 4-15-2: ICMPv6 Ping Page Screenshot

The page includes the following fields:

Object	Description
• **IP Address**	The destination IP Address.
• **Ping Length**	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
• **Ping Count**	The count of the ICMP packet. Values range from 1 time to 60 times.
• **Ping Interval**	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Button

Start: Click to start transmitting ICMP packets.

New Ping: Click to re-start diagnostics with PING.

4.15.3 Remote IP Ping Test

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues on special port.

After you press "**Test**", 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-15-3 appears.

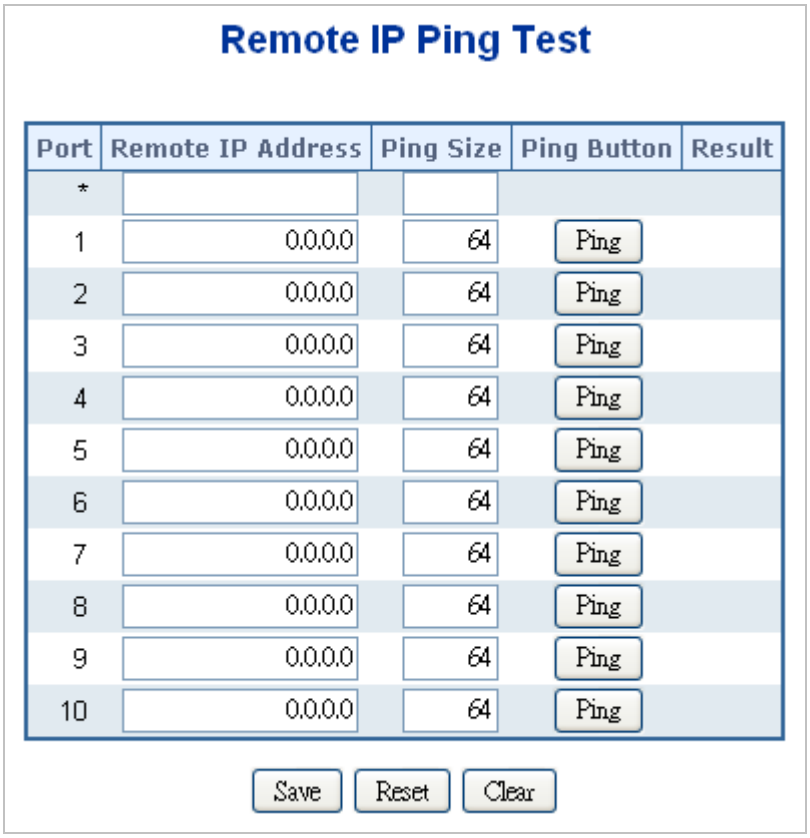


Figure 4-15-3: Remote IP Ping Test Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The logical port for the settings.
• **Remote IP Address**	The destination IP Address.
• **Ping Size**	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.
• **Result**	Display the ping result.

Buttons

Ping: Click to start ping process.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Clear: Clears the local counters. All counters (including global counters) are cleared upon reboot.

4.15.4 Cable Diagnostics

This page is used for running the Cable Diagnostics.

Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running cable diagnostic. Therefore, running cable diagnostic on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete. The ports belong to the currently selected stack unit, as reflected by the page header. The VeriPHY Cable Diagnostics screen in Figure 4-15-4 appears.

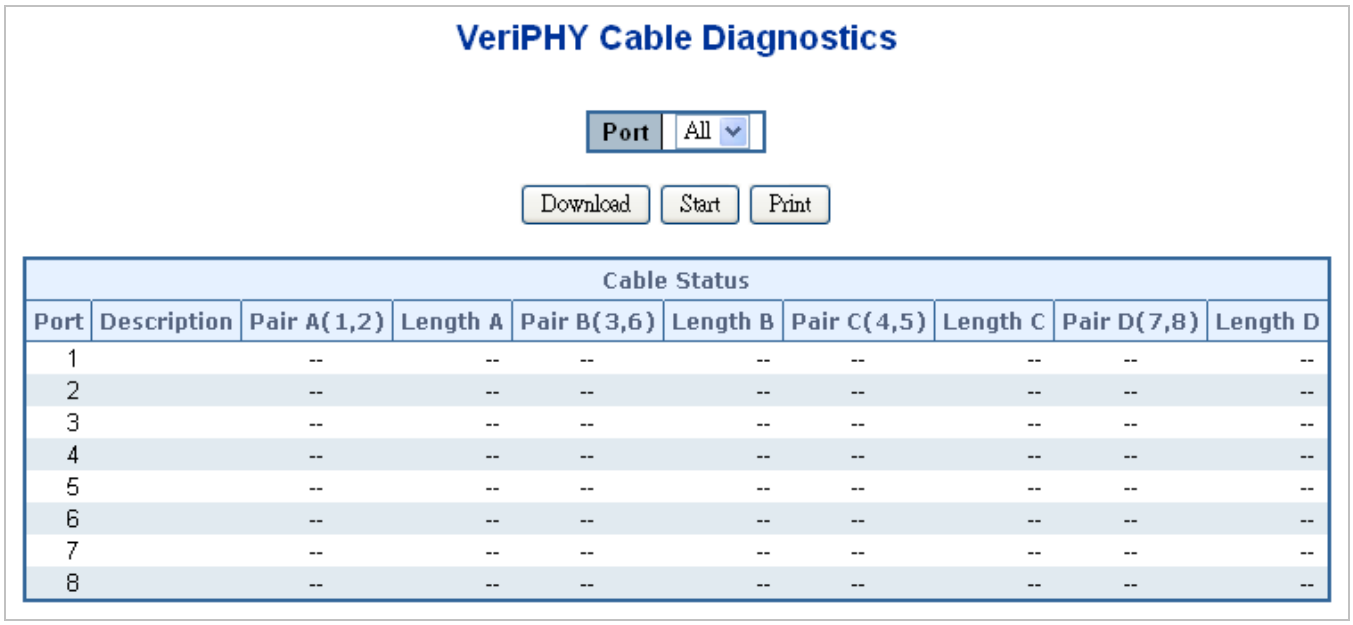

VeriPHY Cable Diagnostics
Port
All
Download
Start
Print
Cable Status
Port Description Pair A(1,2) Length A Pair B(3,6) Length B Pair C(4,5) Length C Pair D(7,8) Length D
1 -- -- -- -- -- -- -- --
2 -- -- -- -- -- -- -- --
3 -- -- -- -- -- -- -- --
4 -- -- -- -- -- -- -- --
5 -- -- -- -- -- -- -- --
6 -- -- -- -- -- -- -- --
7 -- -- -- -- -- -- -- --
8 -- -- -- -- -- -- -- --

Figure 4-15-4: VeriPHY Cable Diagnostics Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The port where you are requesting Cable Diagnostics. Please be noticed that it is only affect to copper port, not fiber port.
• **Cable Status**	**Port**: Port number. **Pair**: The status of the cable pair. **Length**: The length (in meters) of the cable pair.

Buttons

Start: Click to run the diagnostics.

4.16 Power over Ethernet

Providing up to 8 PoE, in-line power interfaces, the NS3552-8P-2S PoE Switch can easily build a power central-controlled IP phone system, IP Camera system, AP group for the enterprise. For instance, 8 camera / AP can be easily installed around the corner in the company for surveillance demands or build a wireless roaming environment in the office. Without the power-socket limitation, the NS3552-8P-2S PoE Switch makes the installation of cameras or WLAN AP more easily and efficiently.

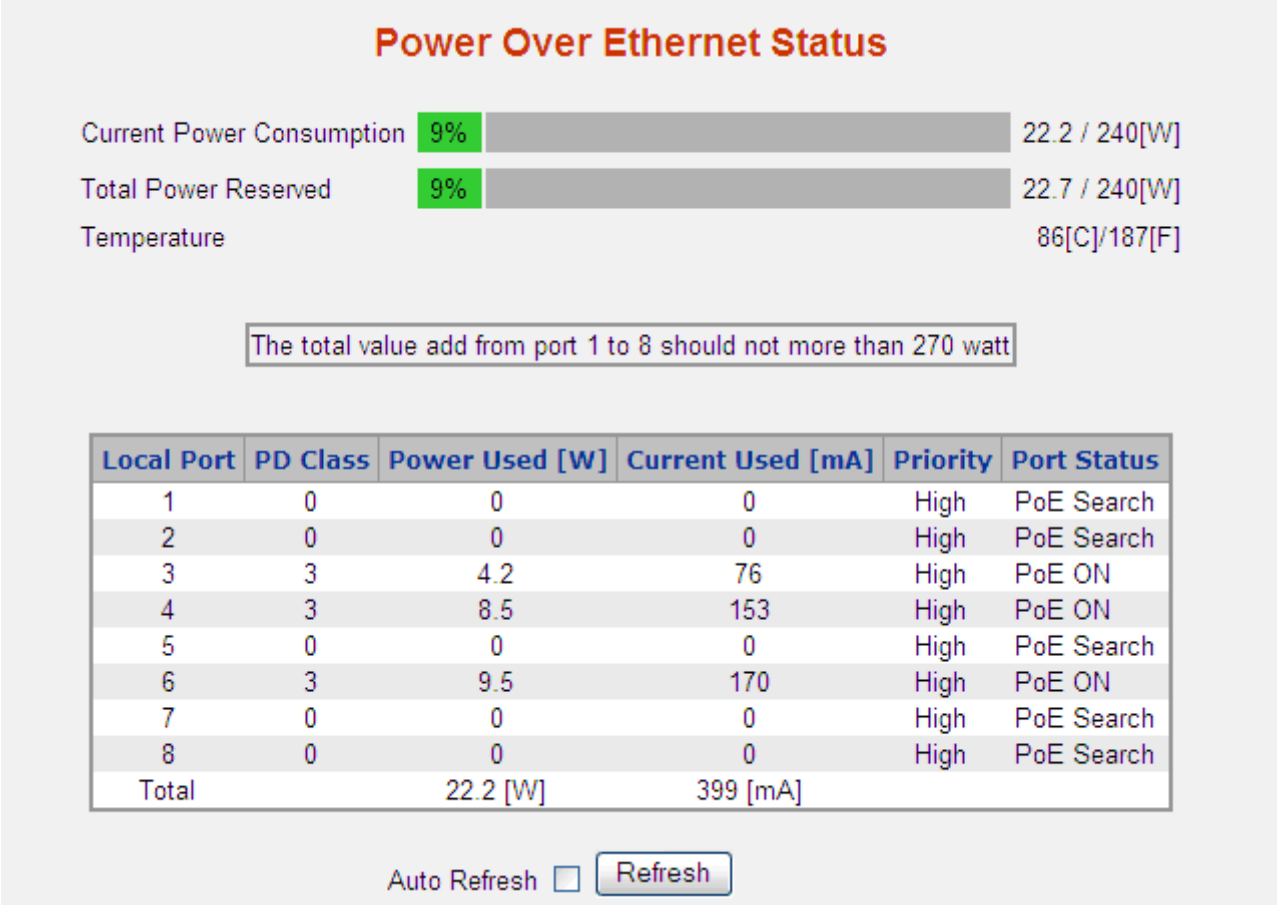

Power Over Ethernet Status
Current Power Consumption
9%
22.2 / 240[W]
Total Power Reserved
9%
22.7 / 240[W]
Temperature
86[C]/187[F]
The total value add from port 1 to 8 should not more than 270 watt
Local Port
PD Class
Power Used [W]
Current Used [mA]
Priority
Port Status
1 0 0 0 High PoE Search
2 0 0 0 High PoE Search
3 3 4.2 76 High PoE ON
4 3 8.5 153 High PoE ON
5 0 0 0 High PoE Search
6 3 9.5 170 High PoE ON
7 0 0 0 High PoE Search
8 0 0 0 High PoE Search
Total 22.2 [W] 399 [mA]
Auto Refresh
Refresh

Figure 4-16-1: Power over Ethernet Status

4.16.1 Power over Ethernet Powered Device

 3~5 Watts	**Voice over IP phones** Enterprise can install POE VoIP Phone, ATA and other Ethernet/non-Ethernet end-devices to the central where UPS is installed for un-interrupt power system and power control system.
 6~12 Watts	**Wireless LAN Access Points** Museum, Sightseeing, Airport, Hotel, Campus, Factory, and Warehouse can install the Access Point anywhere with no hesitation.
 10~12 Watts	**IP Surveillance** Enterprise, Museum, Campus, Hospital, Bank, can install IP Camera without limits of install location – no need electrician to install AC sockets.
 3~12 Watts	**PoE Splitter** PoE Splitter split the PoE 52V DC over the Ethernet cable into 5/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
 3~25 Watts	**High Power PoE Splitter** High PoE Splitter split the PoE 52V DC over the Ethernet cable into 24/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
 30 Watts	**High Power Speed Dome** This state-of-the-art design is considerable to fit in various network environments like traffic centers, shopping malls, railway stations, warehouses, airports, and production facilities for the most demanding outdoor surveillance applications- no need electrician to install AC sockets.

4.16.2 System Configuration

In a power over Ethernet system, operating power is applied from a power source (PSU-power supply unit) over the LAN infrastructure to **powered devices (PDs)**, which are connected to ports. Under some conditions, the total output power required by PDs can exceed the maximum available power provided by the PSU. The system may a prior be planned with a PSU capable of supplying less power than the total potential power consumption of all the PoE ports in the system. In order to maintain the majority of ports active, power management is implemented.

The PSU input power consumption is monitored by measuring voltage and current .The input power consumption is equal to the system's aggregated power consumption .The power management concept allows all ports to be active and activates additional ports, as long as the aggregated power of the system is lower than the power level at which additional PDs cannot be connected .When this value is exceeded, ports will be deactivated, according to user-defined priorities. The power budget is managed according to the following user-definable parameters: maximum available power, ports priority, maximum allowable power per port.

Reserved Power determined by

There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports.

- **Classification mode**

  In this mode each port automatic determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 and 30.8 Watts.

Class	Usage	Range of maximum power used by the PD	Class Description
0	Default	0.44 to 12.95 Watts	Classification unimplemented
1	Optional	0.44 to 3.84 Watts	Very low power
2	Optional	3.84 to 6.49 Watts	Low power
3	Optional	6.49 to 12.95 Watts (or to 15.4Watts)	Mid power
4	Optional	12.95 to 25.50 Watts (or to 30.8Watts)	High power (NS3552-8P-2S Supports Only)

In this mode the **Maximum Power fields** have no effect.

- **Allocation mode**

  In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. The ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver.

In this mode the port power is not turned on if the PD requests more available power.

- **Consumption mode**

  In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

- **Priority mode**

  In this mode the user assign the priority to the ports/PD. When the total PoE power consumption request is over the allowed power supply limitation, the system shut down PoE ports by port priority setting.

Power over Ethernet Configuration

This section allows the user to inspect and configure the current PoE configuration settings; screen in Figure 4-16-2 appears.

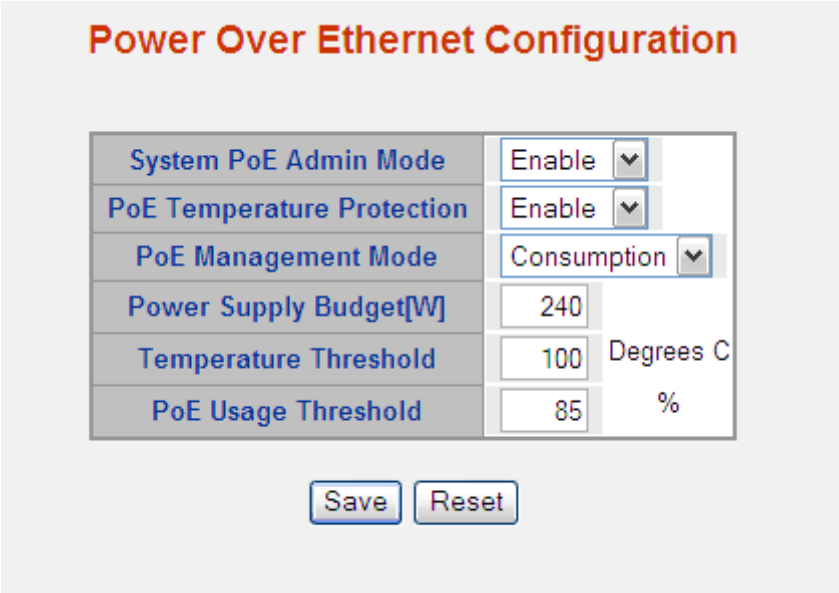


Figure 4-16-2: PoE Configuration Screenshot

The page includes the following fields:

Object	Description
• **System PoE Admin Mode**	Allows user to enable or disable PoE function. It will cause all of PoE ports to supply or not supply power.
• **PoE Temperature Protection**	Allows user to enable or disable PoE Temperature Protection.
• **PoE Management Mode**	There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports. ■ **Classification mode:** System reserves PoE power to PD according to PoE class level. ■ **Allocation mode**: allows user to assign PoE power to per port. ■ **Consumption mode**: System offers PoE power according to PD real power consumption. ■ **Priority mode**: System offers PoE power according to per port priority setting when power consumption has been over total power budget. The default PoE management mode is "**Consumption mode**".
• **Power Supply Budget [W]**	Set limit value of the total PoE port provided power to the PDs. For **NS3552-8P-2S**, the available max. Value is **240** (depends on power input).

• **Temperature Threshold**	Allows setting over temperature protection threshold value. If system temperature is over than the threshold, the system will lower total PoE power budget automatically.
• **PoE Usage Threshold**	Allows setting how much PoE power budget could be limited.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

For **NS3552-8P-2S**, the total PoE power reservation from Port-1~8 is up to **270 watts.**

PD Classifications

A PD may be classified by the PSE based on the classification information provided by the PD. The intent of PD classification is to provide information about the maximum power required by the PD during operation. **Class 0** is the default for PDs. However, to improve power management at the PSE, the PD may opt to provide a signature for **Class 1 to 4**.

The PD is classified based on power. The classification of the PD is the maximum power that the PD will draw across all input voltages and operational modes.

A PD shall return Class 0 to 4 in accordance with the maximum power draw as specified by Table 4-16-1.

Class	Usage	Range of maximum power used by the PD	Class Description
0	Default	0.44 to 12.95 Watts	Classification unimplemented
1	Optional	0.44 to 3.84 Watts	Very low power
2	Optional	3.84 to 6.49 Watts	Low power
3	Optional	6.49 to 12.95 Watts (or to 15.4Watts)	Mid power
4	Optional	12.95 to 25.50 Watts (or to 30.8Watts)	High power

Table 4-16-1 Device class

4.16.3 Port Configuration

This section allows the user to inspect and configure the current PoE port settings; screen in Figure 4-16-3 appears.

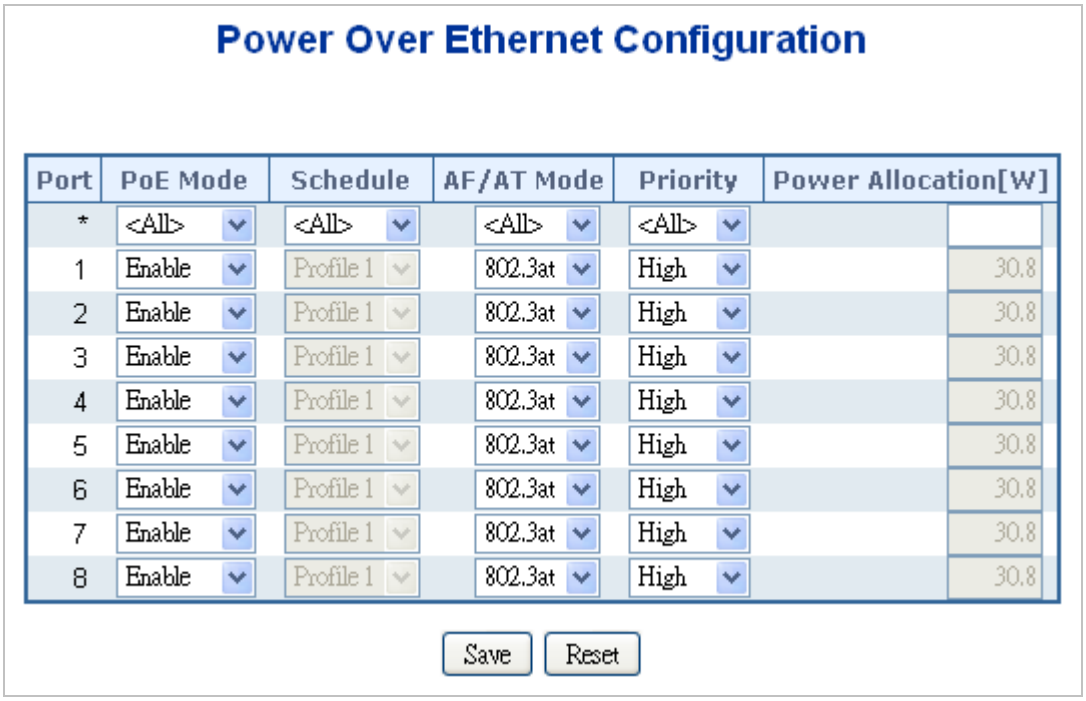

Power Over Ethernet Configuration
Port
PoE Mode
Schedule
AF/AT Mode
Priority
Power Allocation[W]
* <All> <All> <All> <All>
1 Enable Profile 1 802.3at High 30.8
2 Enable Profile 1 802.3at High 30.8
3 Enable Profile 1 802.3at High 30.8
4 Enable Profile 1 802.3at High 30.8
5 Enable Profile 1 802.3at High 30.8
6 Enable Profile 1 802.3at High 30.8
7 Enable Profile 1 802.3at High 30.8
8 Enable Profile 1 802.3at High 30.8
Save
Reset

Figure 4-16-3: Power over Ethernet Configuration Screenshot

The page includes the following fields:

Object	Description
• **PoE Mode**	There are three modes for PoE mode. ■ **Enable**: enable PoE function.. ■ **Disable**: disable PoE function. ■ **Schedule**: enable PoE function in schedule mode.
• **Schedule**	Indicates the schedule profile mode. Possible porifles are: ■ **Profile1** ■ **Profile2** ■ **Profile3** ■ **Profile4**
• **AF/AT Mode**	Allows user to select 802.3at or 802.3af compatibility mode. The default value is 802.3at mode. This function will affect PoE power reservation on Classification power limit mode only as 802.3af mode and system are going to reserve a maximum of 15.4W for PD that supports Class3 level. IEEE 802.3at mode and system are going to reserve 30.8 watts for PD that supports Class4 level. Class1 to class3 level in the 802.3at mode will reserve the same PoE power in the 802.3af mode.
• **Priority**	The Priority represents PoE ports priority. There are three levels of power priority named **Low**, **High** and **Critical**. The priority is used in the case when total power consumption has been over total power budget. In this case the port with the lowest priority will be turned off, and offer power for the port of higher priority.
• **Power Allocation**	It can limit the port PoE supply watts. Per port maximum value must be less than **15.4** / **30.8 watts**, and total ports values must be less than the Power Reservation value. Once power overload is detected, the port will auto shut down and keep on detection mode until PD's power consumption is lower than the power limit value NS3552-8P-2S = 30.8 watts for per port PoE output

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.16.4 PoE Status

This page allows the user to inspect the total power consumption and total power reserved and current status for all PoE ports.

The screen in Figure 4-16-4 appears.

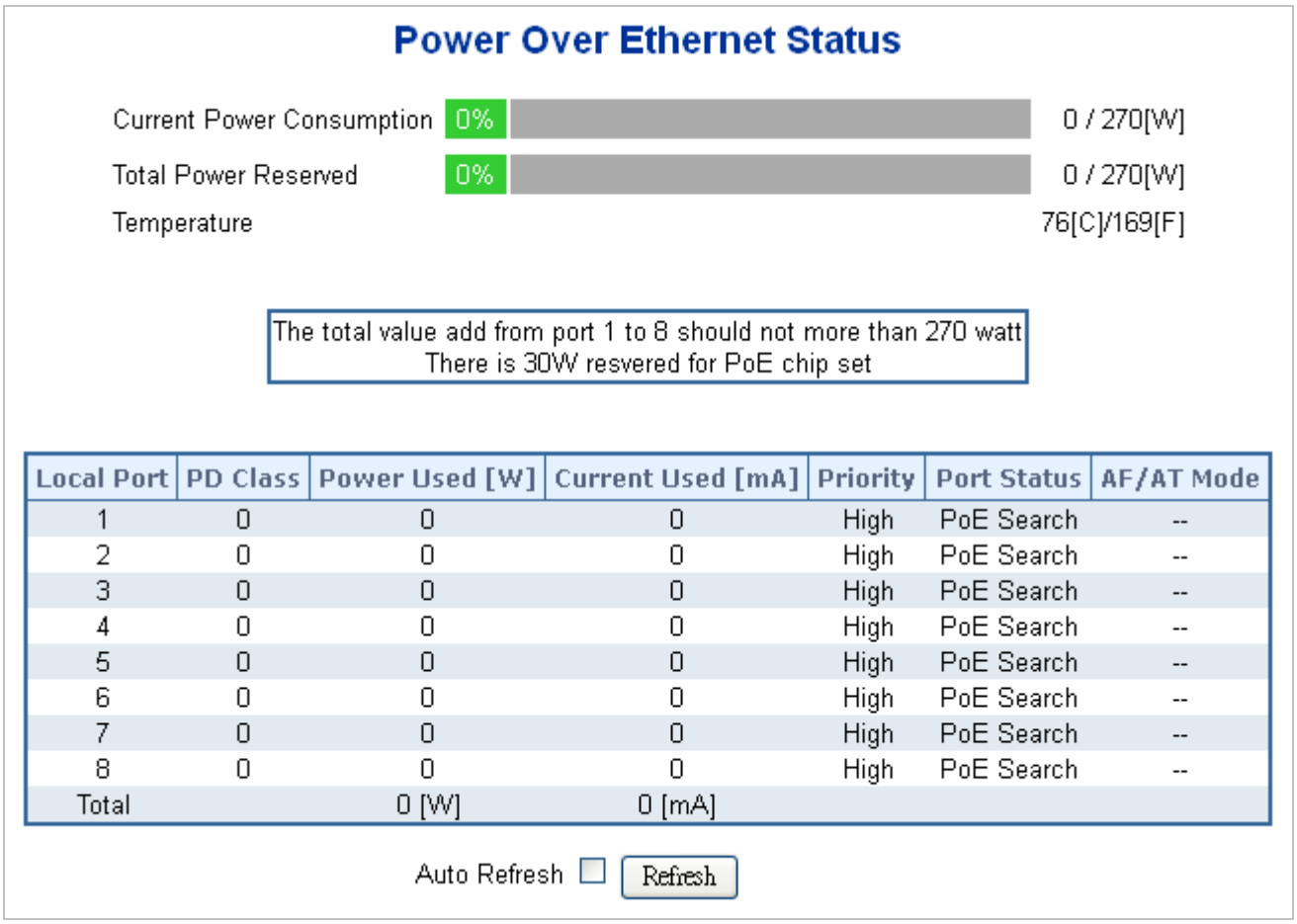

Power Over Ethernet Status
Current Power Consumption
0%
0 / 270[W]
Total Power Reserved
0%
0 / 270[W]
Temperature
76[C]/169[F]
The total value add from port 1 to 8 should not more than 270 watt
There is 30W resvered for PoE chip set
Local Port
PD Class
Power Used [W]
Current Used [mA]
Priority
Port Status
AF/AT Mode
1 0 0 0 High PoE Search --
2 0 0 0 High PoE Search --
3 0 0 0 High PoE Search --
4 0 0 0 High PoE Search --
5 0 0 0 High PoE Search --
6 0 0 0 High PoE Search --
7 0 0 0 High PoE Search --
8 0 0 0 High PoE Search --
Total 0 [W] 0 [mA]
Auto Refresh
Refresh

Figure 4-16-4: PoE Status Screenshot

The page includes the following fields:

Object	Description
• **Current Power Consumption**	Show the total watts usage of Managed PoE Switch.
• **Total Power Reserved**	Shows how much the total power is reserved for all PDs.
• **Temperature 1**	Display the current operating temperature of the first PoE chip unit.
• **Temperature 2**	Display the current operating temperature of the second PoE chip unit.
• **Local Port**	This is the logical port number for this row.

• **PD Class**	Display the class of the PD attached to the port, as established by the classification process. Class 0 is the default for PDs. The PD is powered based on PoE Class level if system working on Classification mode. A PD shall return Class 0 to 4 in accordance with the maximum power draw as specified by **Table 4-16-1**.
• **Power Used [W]**	The **Power Used** shows how much power the PD currently is using.
• **Current Used [mA]**	The **Power Used** shows how much current the PD currently is using.
• **Priority**	The **Priority** shows the port's priority configured by the user.
• **Port Status**	The **Port Status** shows the port's status.
• **AF / AT Mode**	Display per PoE port operates at 802.3af or 802.3at mode. (NS3552-8P-2S Supports Only)
• **Total**	Show the total power and current usage of all PDs.

Buttons

Auto-refresh : Check this box to enable an automatic refresh of the page at regular intervals.

Refresh: Click to refresh the page immediately.

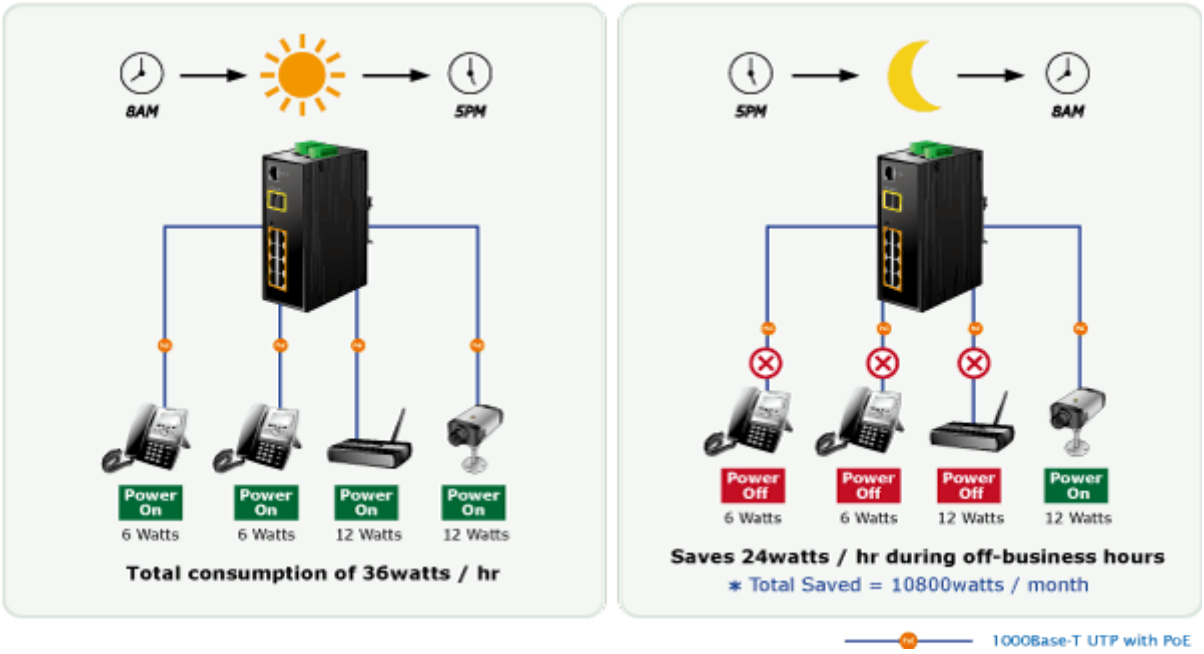
4.16.5 PoE Schedule

The PoE Schedule of the NS3552-8P-2S features two advanced PD power control functions:

- **PD power ON/OFF Schedule**
- **Schedule Power Recycle**

PD Power ON/OFF Schedule

Under the trend of energy saving worldwide and contribute to environment protection on the earth, the NS3552-8P-2S can effectively control the power supply besides its capability of giving high watts power. The "**PoE schedule**" function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMB or Enterprise save power and money.



Schedule Power Recycle

The NS3552-8P-2S allows each of the connected PoE powered device to reboot in a specific time each week. Therefore, it will reduce the chance of powered device crash resulting from buffer overflow.

■ Power over Ethernet Schedule Configuration

This page allows the user to define PoE schedule. The screen in Figure 4-16-5 appears.

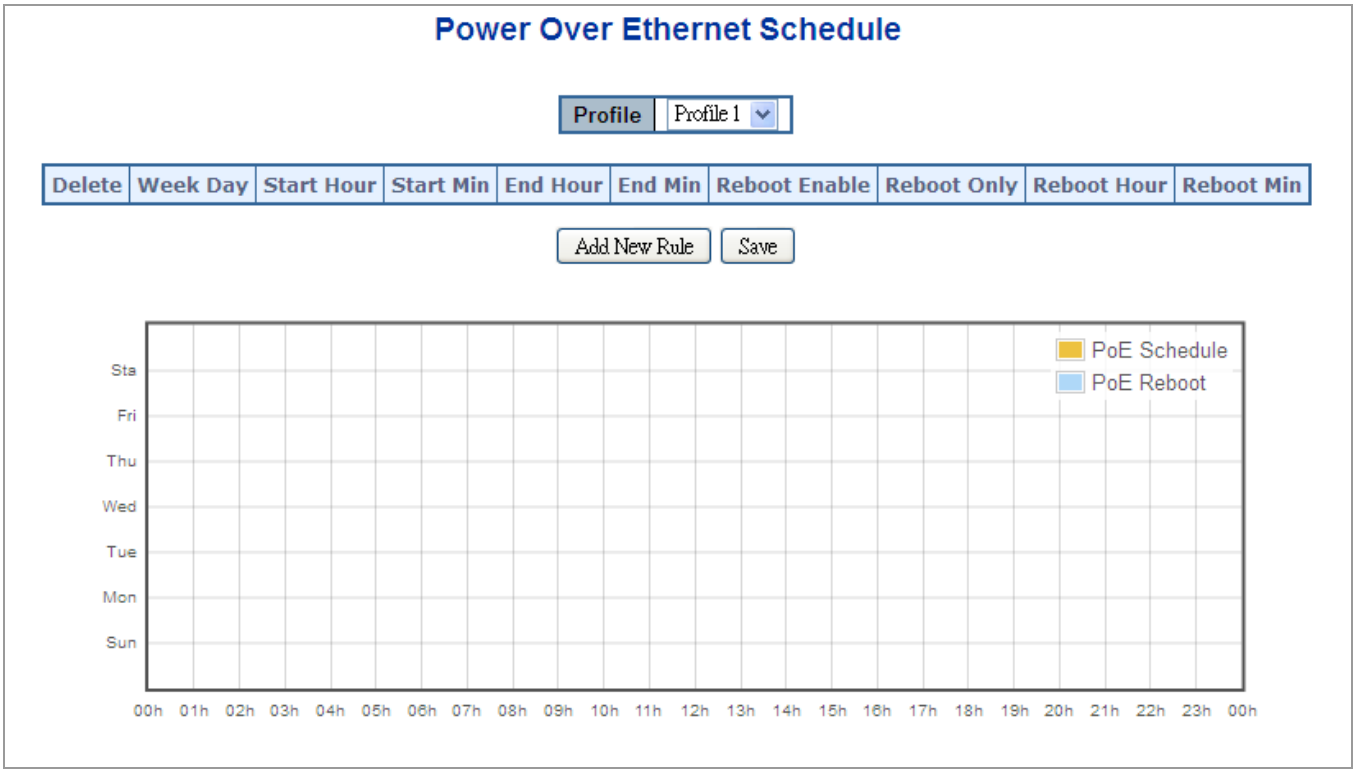


Figure 4-16-5: PoE Schedule Screenshot

Please press **Add New Rule** button to start set PoE Schedule function. You have to set PoE schedule to profile, then go back to PoE Port Configuration, and select "**Schedule**" mode from per port "PoE Mode" option. Then you can indicate which schedule profile could be applied to the PoE port.

The page includes the following fields:

Object	Description
• **Profile**	Set the schedule profile mode. Possible profiles are: **Profile1** **Profile2** **Profile3** **Profile4**
• **Week Day**	Allows user to set week day for defining PoE function, which should be enabled on the day.
• **Start Hour**	Allows user to set at what hour that best enables PoE function.
• **Start Min**	Allows user to set at what minute that best enables PoE function.
• **End Hour**	Allows user to set at what hour that best disables PoE function.
• **End Min**	Allows user to set at what minute that best disables PoE function.
• **Reboot Enable**	Allows user to enable or disable whole PoE port reboot by PoE reboot schedule. Please be noted that if you want PoE schedule and PoE reboot schedule to work at the same time, please use this function, and don't use **Reboot Only** function. This function offers administrator to reboot PoE device at an indicated time if administrator has this kind of requirement.

• **Reboot Only**	Allows user to reboot PoE function by PoE reboot schedule. Please be noted that if administrator enables this function, PoE schedule will not set time to profile. This function is just only for PoE port reset at the indicated time.
• **Reboot Hour**	Allows user to set at what hour that best reboots PoE. This function is only for PoE reboot schedule.
• **Reboot Min**	Allows user to set at what minute that best reboot PoE. This function is only for PoE reboot schedule.

Buttons

Add New Rule: click to add new rule.

Save: Click to save changes.

Delete: Check to delete the entry.

4.16.6 LLDP PoE Neighbors

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected. The columns hold the following information: The screen in Figure 4-16-6 appears.

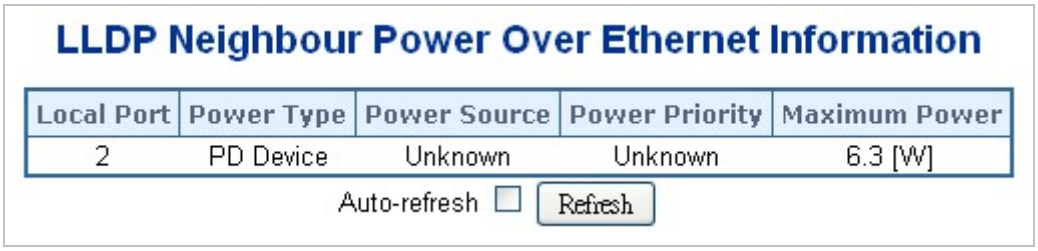


Figure 4-16-6: LLDP PoE Neighbor Screenshot

Please be noted that administrator has to enable LLDP port from LLDP configuration. Please refer to the following example as shown in Figure 4-16-7. If LLDP function from port1 to port3 is enabled, administrator has to plug a PD that supports PoE LLDP function, and then administrator is going to see the PoE information of the PD from LLDP.

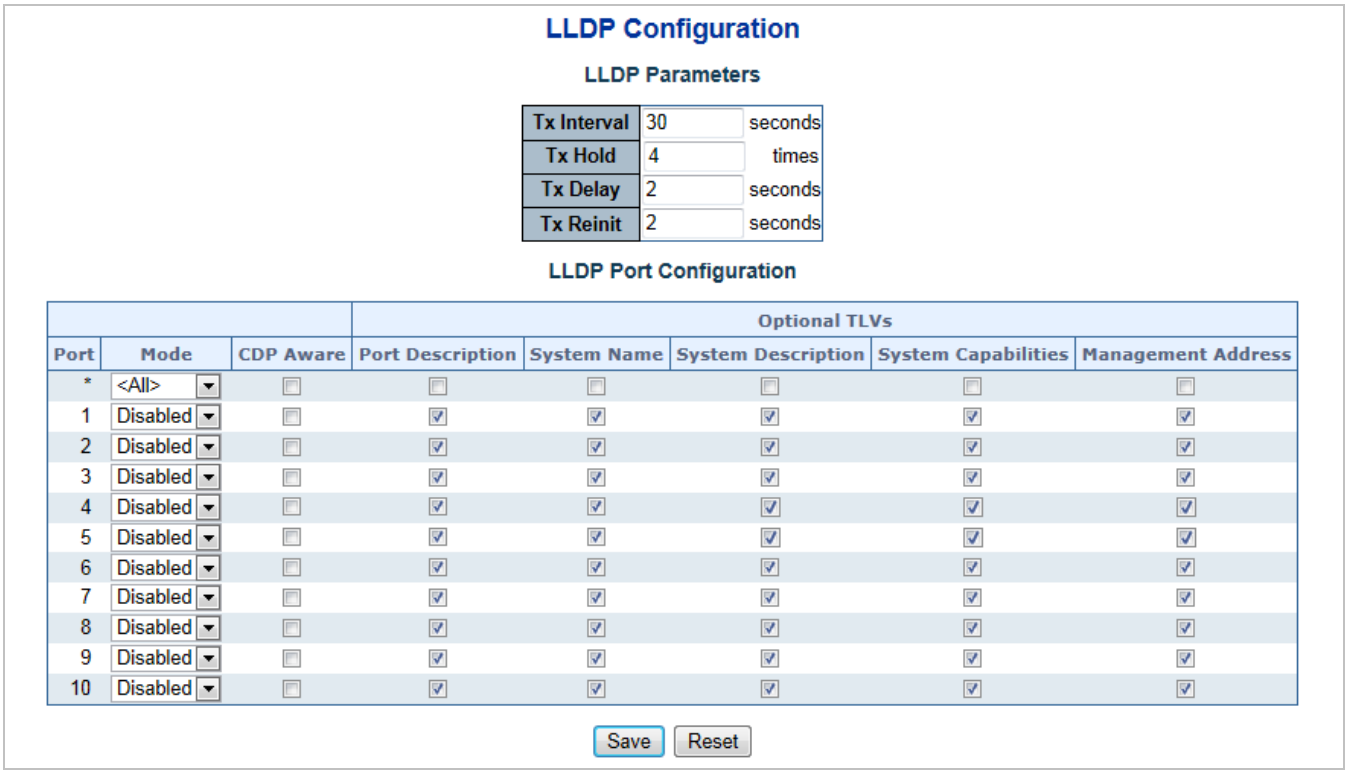


Figure 4-16-7: LLDP Configuration Screenshot

4.16.7 PoE Alive Check Configuration

The NS3552-8P-2S PoE Switch can be configured to monitor connected PD's status in real time via ping action. Once the PD stops working and is without response, the NS3552-8P-2S PoE Switch is going to restart PoE port power, and bring the PD back to work. It will greatly enhance the reliability and reduces administrator management burden.

■ PD Ping Alive Check Configuration

This page provides you with how to configure PD Alive Check. The screen in Figure 4-16-8 appears.

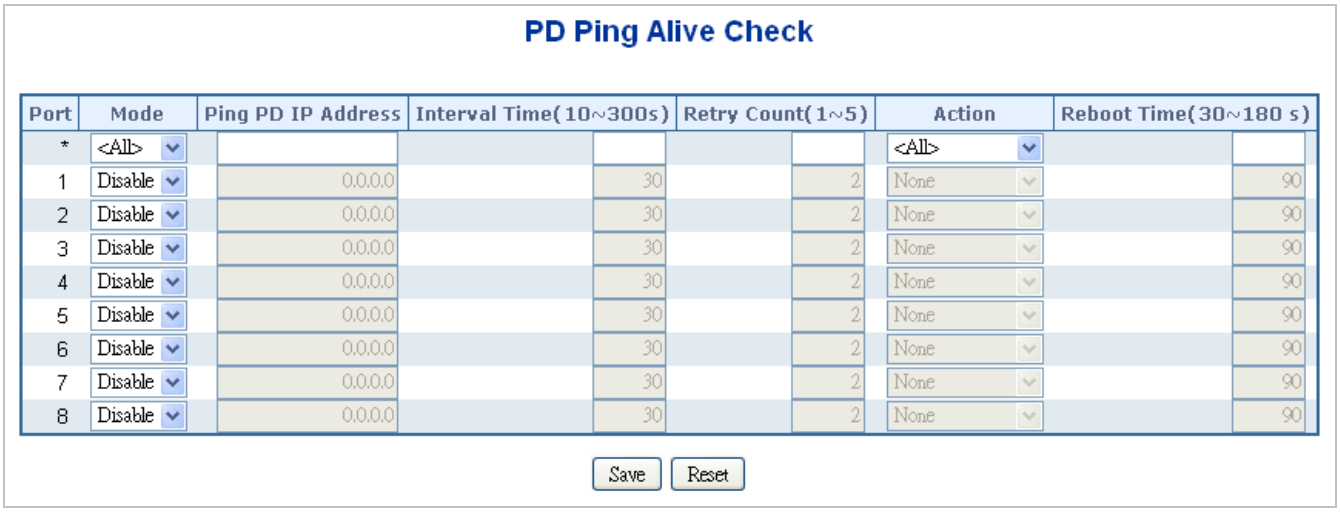


Figure 4-16-8: PD Alive Check Configuration Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Allows user to enable or disable per port PD Alive Check function. As default value all ports are disabled.
• **Ping PD IP Address**	This column allows user to set PoE device IP address here for system making ping to the PoE device. Please be noted that the PD's IP address must be set to the same network segment as the NS3552-8P-2S PoE Switch.
• **Interval Time (10~300s)**	This column allows user to set how long system should issue a ping request to PD for detecting PD whether it is alive or dead. Interval time range is from 10 seconds to 300 seconds.
• **Retry Count (1~5)**	This column allows user to set how many times system retries ping to PD. For example, if we set count 2, the meaning is that if system retries ping to the PD and the PD doesn't response continuously, the PoE port will be reset.
• **Action**	Allows user to set which action will be applied if the PD is without any response. The NS3552-8P-2S PoE Switch offers 3 actions as follows: ➢ **PD Reboot:** It means system will reset the PoE port that is connected to the PD.

	➢ **Reboot & Alarm:** It means system will reset the PoE port and issue an alarm message via Syslog, SMTP. ➢ **Alarm:** It means system will issue an alarm message via Syslog, SMTP.
• **Reboot Time (30~180s)**	This column allows user to set the PoE device rebooting time, due to there is so many kinds of PoE devices on the market and they have different rebooting times. The PD Alive-check is not a defining standard, so the PoE device on the market doesn't report reboots done information to the NS3552-8P-2S PoE Switch, so user has to make sure how long the PD will be finished to boot, and then set the time value to this column. System is going to check the PD again according to the reboot time. If you cannot make sure precisely what booting time is, we suggest you to set it longer.

Buttons

Save: Click it to save changes.

Reset: Click it to reset configuration which doesn't want to be saved yet.

4.17 Loop Protection

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.

4.17.1 Configuration

This page allows the user to inspect the current Loop Protection configurations,

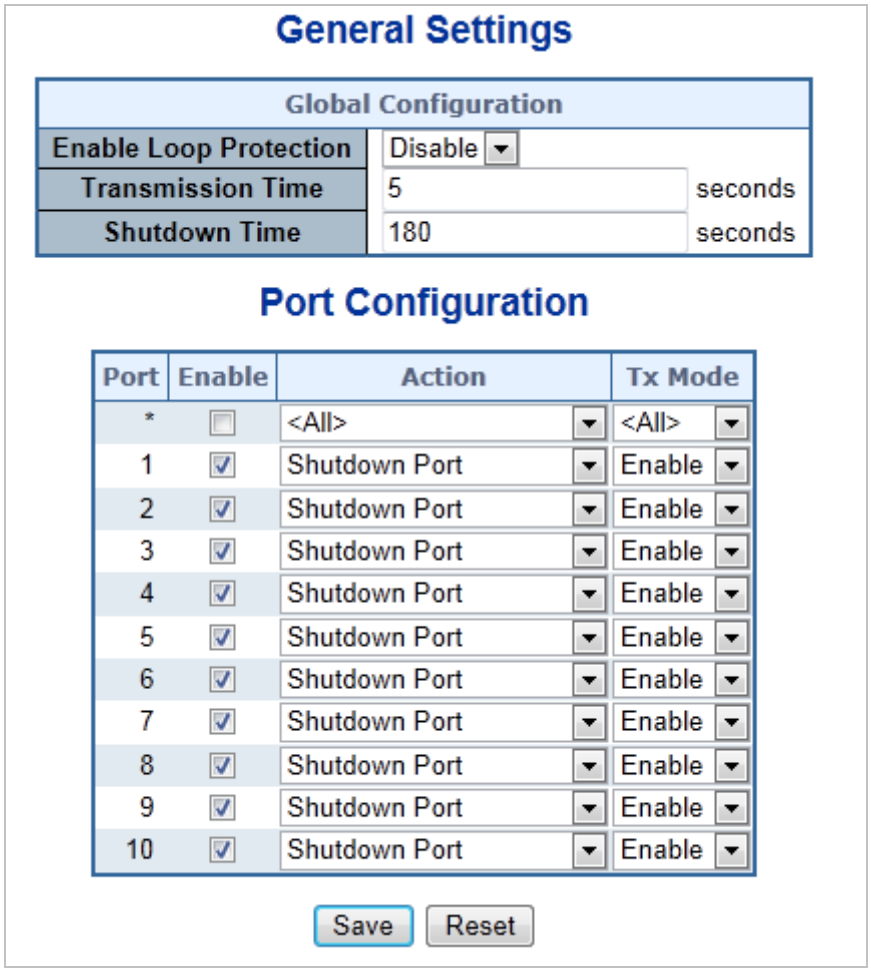


Figure 4-17-1: Loop Protection Configuration Page Screenshot

The page includes the following fields:

General Settings:

Object	Description
• **Enable Loop Protection**	Controls whether loop protections is enabled (as a whole).
• **Transmission Time**	The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.
• **Shutdown Time**	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).

Port Configuration:

Object	Description
• **Port**	The switch port number of the port.
• **Enable**	Controls whether loop protection is enabled on this switch port.
• **Action**	Configures the action performed when a loop is detected on a port. Valid values are **Shutdown Port**, **Shutdown Port and Log** or **Log Only**.
• **Tx Mode**	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.17.2 Status

This page displays the loop protection port status the ports from the Industrial Managed Switch.

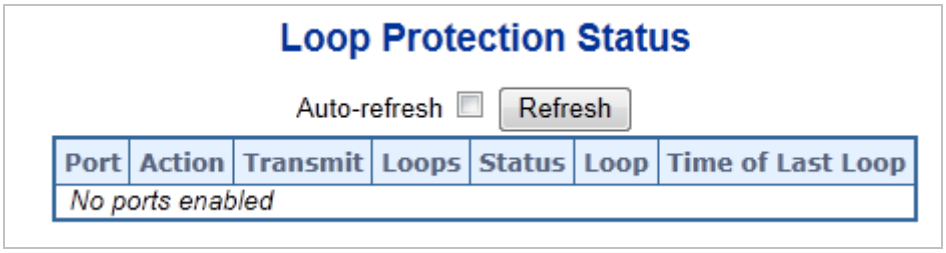


Figure 4-17-2: Loop Protection Status Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	The switch port number of the logical port.
• **Action**	The currently configured port action.
• **Transmit**	The currently configured port transmit mode.
• **Loops**	The number of loops detected on this port.
• **Status**	The current loop protection status of the port.
• **Loop**	Whether a loop is currently detected on the port.
• **Time of Last Loop**	The time of the last loop event detected.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

4.18 RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

MID of RMON consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

- **Statistics:** Maintain basic usage and error statistics for each subnet monitored by the Agent.
- **History:** Record periodical statistic samples available from Statistics.
- **Alarm:** Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.
- **Event:** A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

4.18.1 RMON Alarm Configuration

Configure RMON Alarm table on this page. The entry index key is **ID**.; screen in Figure 4-18-1 appears.

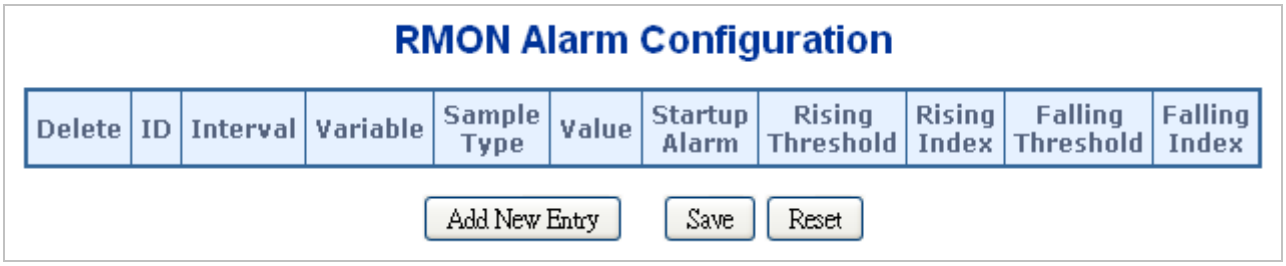


Figure 4-18-1: RMON Alarm configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Interval**	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
• **Variable**	Indicates the particular variable to be sampled, the possible variables are: ■ **InOctets**: The total number of octets received on the interface, including framing characters. ■ **InUcastPkts**: The number of uni-cast packets delivered to a higher-layer protocol. ■ **InNUcastPkts**: The number of broad-cast and multi-cast packets delivered

	to a higher-layer protocol. ■ **InDiscards**: The number of inbound packets that are discarded even the packets are normal. ■ **InErrors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. ■ **InUnknownProtos**: the number of the inbound packets that were discarded because of the unknown or un-support protocol. ■ **OutOctets**: The number of octets transmitted out of the interface, including framing characters. ■ **OutUcastPkts**: The number of uni-cast packets that request to transmit. **OutNUcastPkts**: The number of broad-cast and multi-cast packets that request to transmit. ■ **OutDiscards**: The number of outbound packets that are discarded event the packet is normal. ■ **OutErrors**: The number of outbound packets that could not be transmitted because of errors. ■ **OutQLen**: The length of the output packet queue (in packets).
• **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: ■ **Absolute**: Get the sample directly. ■ **Delta**: Calculate the difference between samples (default).
• **Value**	The value of the statistic during the last sampling period.
• **Startup Alarm**	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: ■ **Rising**Trigger alarm when the first value is larger than the rising threshold. ■ **Falling**Trigger alarm when the first value is less than the falling threshold. ■ **RisingOrFalling**Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
• **Rising Threshold**	Rising threshold value (-2147483648-2147483647).
• **Rising Index**	Rising event index (1-65535).
• **Falling Threshold**	Falling threshold value (-2147483648-2147483647)
• **Falling Index**	Falling event index (1-65535).

Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.18.2 RMON Alarm Status

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table; screen in Figure 4-18-2 appears.

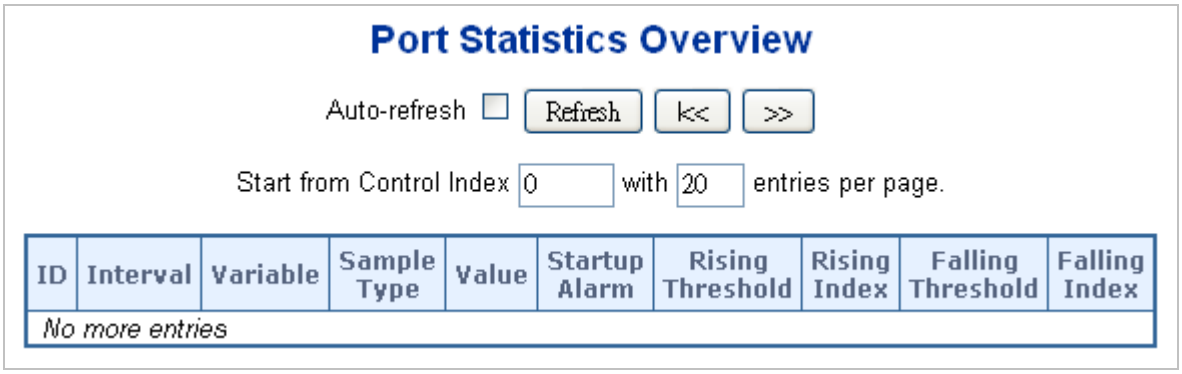


Figure 4-18-2: Port Statistics Overview page screenshot

The page includes the following fields:

Object	Description
• **ID**	Indicates the index of Alarm control entry.
• **Interval**	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
• **Variable**	Indicates the particular variable to be sampled
• **Sample Type**	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
• **Value**	The value of the statistic during the last sampling period.
• **Startup Alarm**	The alarm that may be sent when this entry is first set to valid.
• **Rising Threshold**	Rising threshold value.
• **Rising Index**	Rising event index.
• **Falling Threshold**	Falling threshold value.
• **Falling Index**	Falling event index.

Buttons

Auto-refresh ☐: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.18.3 RMON Event Configuration

Configure RMON Event table on this page. The entry index key is **ID**; screen in Figure 4-18-3 appears.

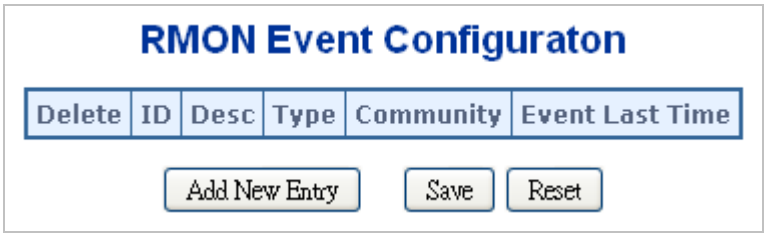


Figure 4-18-3: RMON event configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Desc**	Indicates this event, the string length is from 0 to 127, default is a null string.
• **Type**	Indicates the notification of the event, the possible types are: ■ **none**: The total number of octets received on the interface, including framing characters. ■ **log**: The number of uni-cast packets delivered to a higher-layer protocol. ■ **snmptrap**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. ■ **logandtrap**: The number of inbound packets that are discarded even the packets are normal.
• **Community**	Specify the community when trap is sent, the string length is from 0 to 127, default is "public".
• **Event Last Time**	Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.18.4 RMON Event Status

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table; screen in Figure 4-18-4 appears.

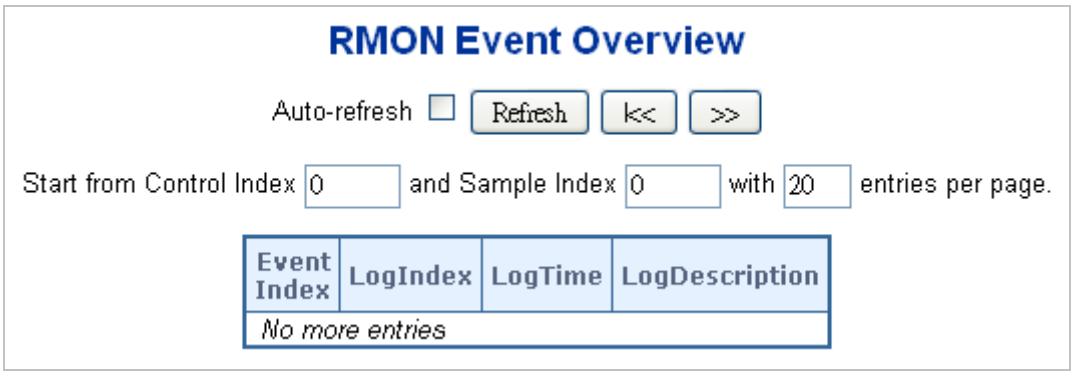


Figure 4-18-4: RMON Event Overview page screenshot

The page includes the following fields:

Object	Description
• **Event Index**	Indicates the index of the event entry.
• **Log Index**	Indicates the index of the log entry.
• **LogTime**	Indicates Event log time
• **LogDescription**	Indicates the Event description.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.18.5 RMON History Configuration

Configure RMON History table on this page. The entry index key is **ID**; screen in Figure 4-18-5 appears.

Figure 4-18-5: RMON history configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Data Source**	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005.
• **Interval**	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
• **Buckets**	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.
• **Buckets Granted**	The number of data shall be saved in the RMON.

Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.18.6 RMON History Status

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table; screen in Figure 4-18-6 appears.

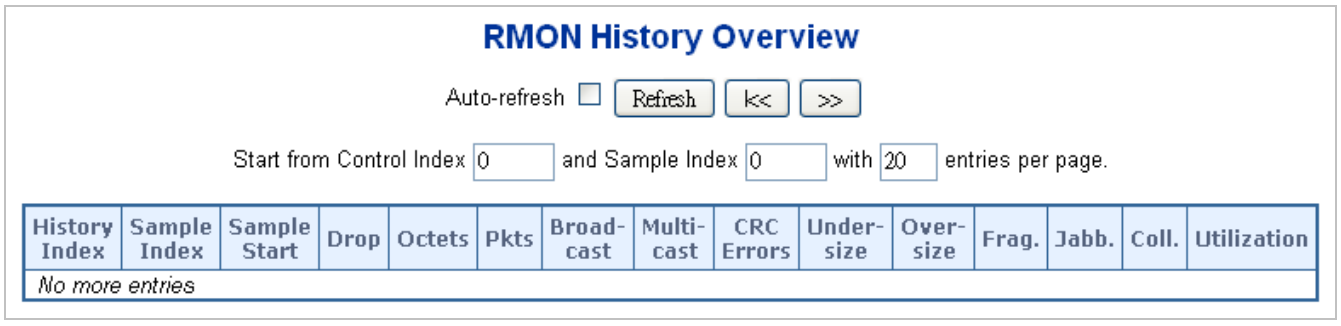


Figure 4-18-6: RMON history overview page screenshot

The page includes the following fields:

Object	Description
• **History Index**	Indicates the index of History control entry.
• **Sample Index**	Indicates the index of the data entry associated with the control entry
• **Sample Start**	The total number of events in which packets were dropped by the probe due to lack of resources.
• **Drops**	The total number of events in which packets were dropped by the probe due to lack of resources.
• **Octets**	The total number of octets of data (including those in bad packets) received on the network.
• **Pkts**	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• **Broadcast**	The total number of good packets received that were directed to the broadcast address.
• **Multicast**	The total number of good packets received that were directed to a multicast address.
• **CRCErrors**	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.
• **Undersize**	The total number of packets received that were less than 64 octets.
• **Oversize**	The total number of packets received that were longer than 1518 octets.
• **Frag.**	The number of frames which size is less than 64 octets received with invalid CRC.
• **Jabb.**	The number of frames which size is larger than 64 octets received with invalid CRC.
• **Coll.**	The best estimate of the total number of collisions on this Ethernet segment.
• **Utilization**	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

<<: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

>>: Updates the table, starting with the entry after the last entry currently displayed.

4.18.7 RMON Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is **ID**; screen in Figure 4-18-7 appears.

Figure 4-18-7: RMON Statistics Configuration Page screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **ID**	Indicates the index of the entry. The range is from 1 to 65535.
• **Data Source**	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.18.8 RMON Statistics Status

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table; screen in Figure 4-18-8 appears.

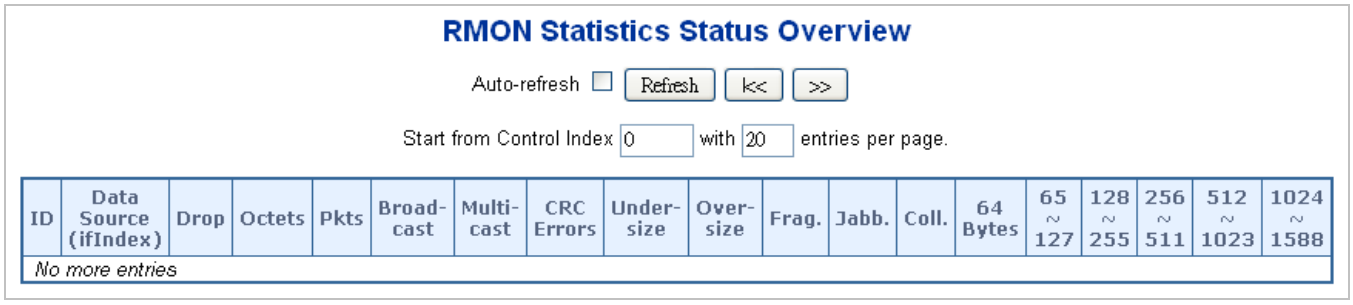


Figure 4-18-8: RMON Statistics Status page screenshot

The page includes the following fields:

Object	Description
• **ID**	Indicates the index of Statistics entry.
• **Data Source (idIndex)**	The port ID which wants to be monitored.
• **Drop**	The total number of events in which packets were dropped by the probe due to lack of resources.
• **Octets**	The total number of octets of data (including those in bad packets) received on the network.
• **Pkts**	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
• **Broad-cast**	The total number of good packets received that were directed to the broadcast address.
• **Multi-cast**	The total number of good packets received that were directed to a multicast address.
• **CRC Errors**	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
• **Under-size**	The total number of packets received that were less than 64 octets.
• **Over-size**	The total number of packets received that were longer than 1518 octets.
• **Frag.**	The number of frames which size is less than 64 octets received with invalid CRC.
• **Jabb.**	The number of frames which size is larger than 64 octets received with invalid CRC.
• **Coll.**	The best estimate of the total number of collisions on this Ethernet segment.
• **64**	The total number of packets (including bad packets) received that were 64 octets in length.
• **65~127**	The total number of packets (including bad packets) received that were from 65 to 127 octets in length.
• **128~255**	The total number of packets (including bad packets) received that were from 128 to 255 octets in length.
• **256~511**	The total number of packets (including bad packets) received that were from 256 to 511 octets in length.
• **512~1023**	The total number of packets (including bad packets) received that were from 512 to 1023 octets in length.
• **1024~1588**	The total number of packets (including bad packets) received that were from 1024 to 1588 octets in length.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 6 seconds.

Refresh: Click to refresh the page immediately.

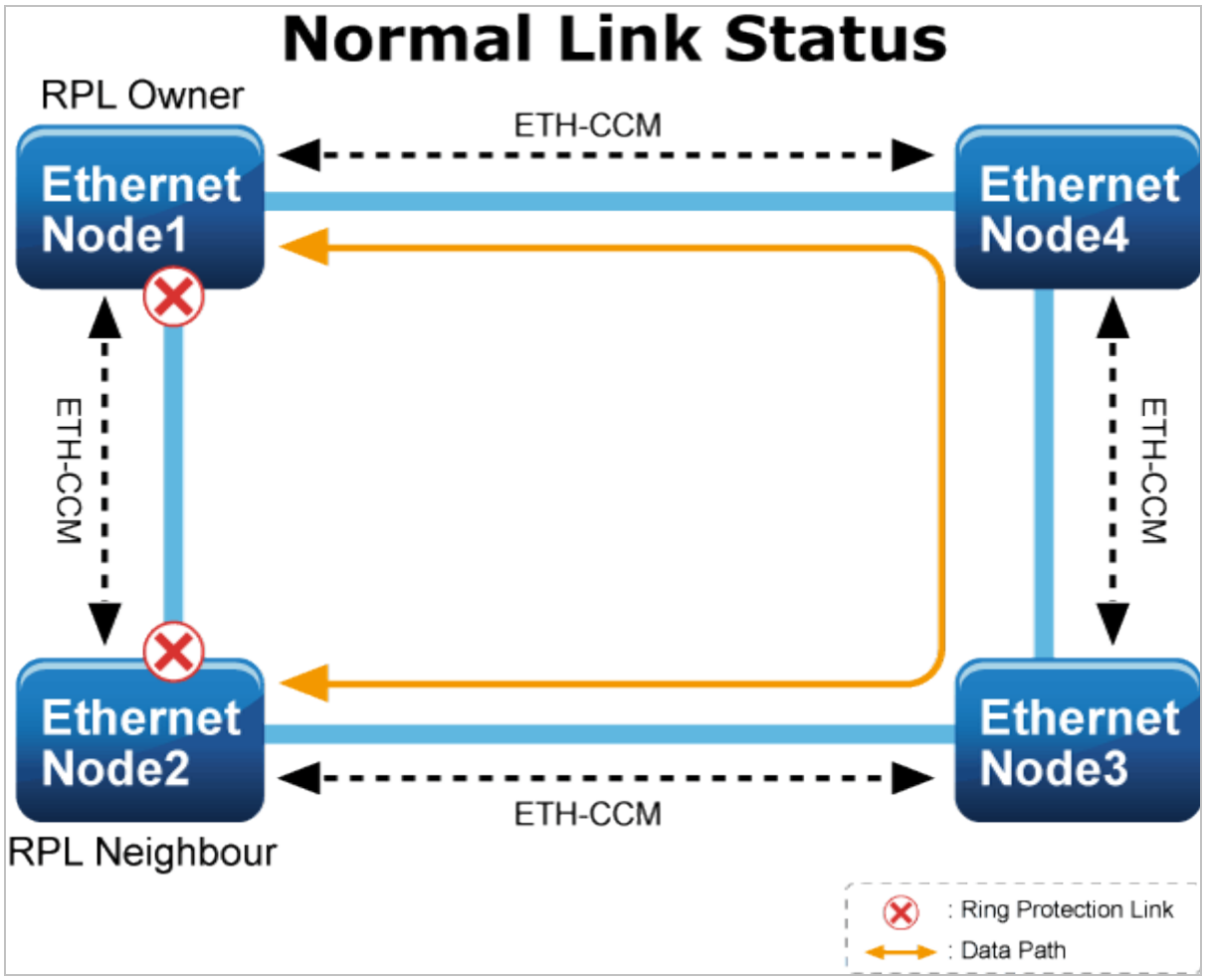
<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.

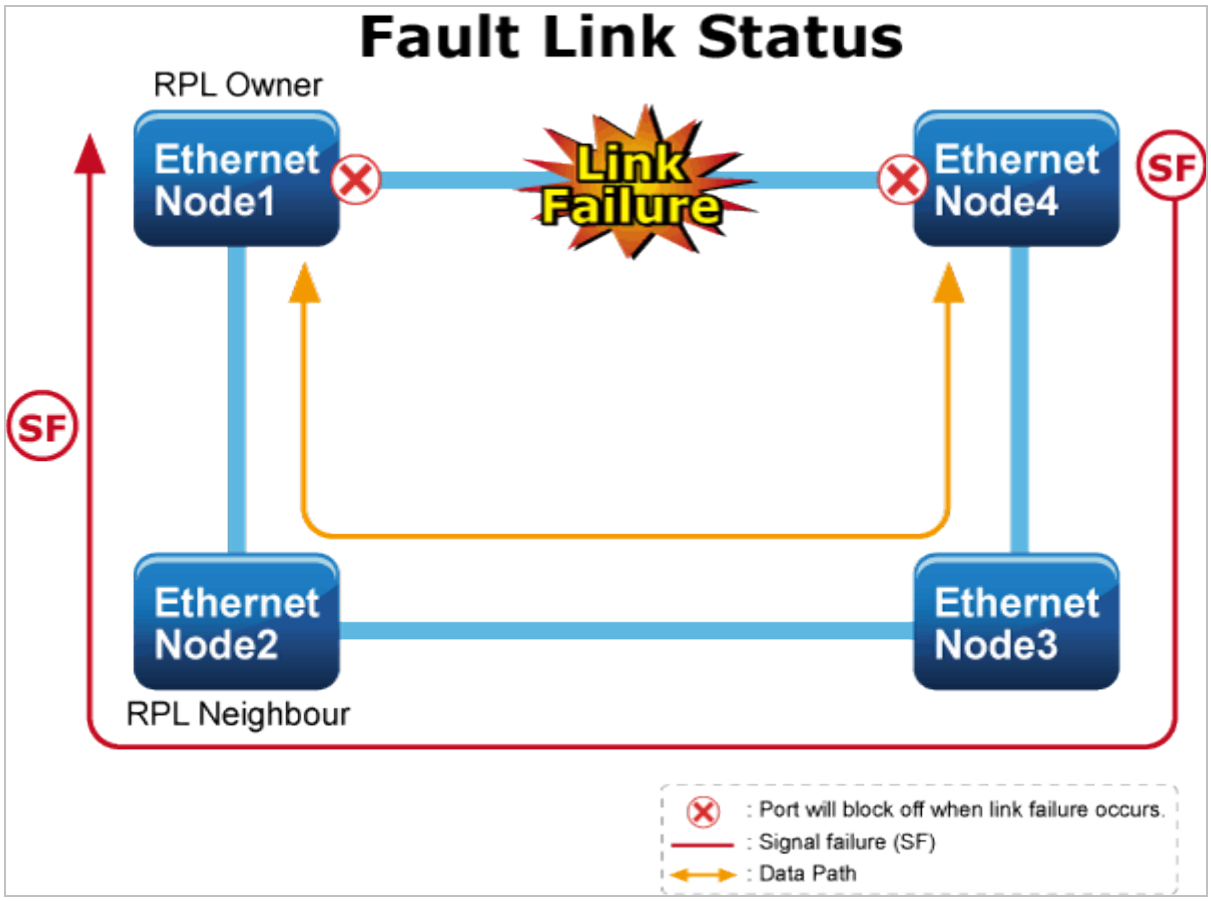
>>: Updates the table, starting with the entry after the last entry currently displayed.

4.19 Ring

ITU-T G.8032 **Ethernet Ring protection switching** (**ERPS**) is a link layer protocol applied on Ethernet loop protection to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology.

ERPS provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the Ring topology, every switch should be enabled with Ring function and two ports should be assigned as the member ports in the ERPS. Only one switch in the Ring group would be set as the RPL owner switch that one port would be blocked, called **owner port**, and PRL neighbor switch has one port that one port would be blocked, called **neighbor port** that connect to owner port directly and this link is called the **Ring Protection Link** or **RPL**. Each switch will sends ETH-CCM message to check the link status in the ring group. When the failure of network connection occurs, the nodes block the failed link and report the signal failure message, the RPL owner switch will automatically unblocks the PRL to recover from the failure.


Normal Link Status
RPL Owner
ETH-CCM
Ethernet Node1
Ethernet Node4
ETH-CCM
ETH-CCM
Ethernet Node2
Ethernet Node3
ETH-CCM
RPL Neighbour
: Ring Protection Link
: Data Path


Fault Link Status
RPL Owner
Ethernet Node1
Link Failure
Ethernet Node4
SF
SF
Ethernet Node2
Ethernet Node3
RPL Neighbour
: Port will block off when link failure occurs.
: Signal failure (SF)
: Data Path

4.19.1 MEP Configuration

The Maintenance Entity Point instances are configured here; screen in Figure 4-19-1 appears.

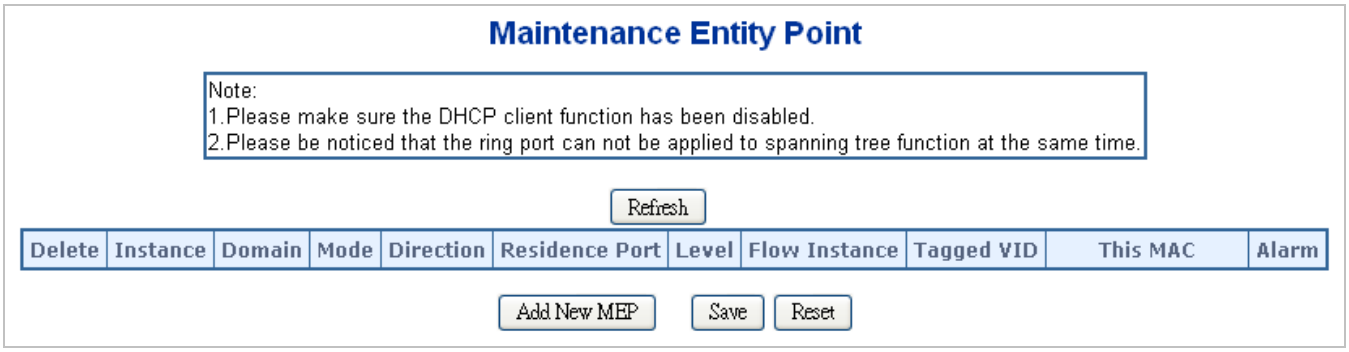


Figure 4-19-1: MEP configuration page screenshot

The page includes the following fields:

Object	Description
• **Delete**	This box is used to mark a MEP for deletion in next Save operation.
• **Instance**	The ID of the MEP. Click on the ID of a MEP to enter the configuration page.
• **Domain**	**Port**: This is a MEP in the Port Domain. 'Flow Instance' is a Port. **Esp**: Future use **Evc**: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC **Mpls**: Future use
• **Mode**	**MEP**: This is a Maintenance Entity End Point. **MIP**: This is a Maintenance Entity Intermediate Point.
• **Direction**	**Ingress**: This is Ingress (down) MEP - monitoring ingress traffic on 'Residence Port'. **Egress**: This is an Egress (up) MEP - monitoring egress traffic on 'Residence Port'.
• **Residence Port**	The port where MEP is monitoring - see 'Direction'.
• **Level**	The MEG level of this MEP.
• **Flow Instance**	The MEP is related to this flow - See 'Domain'.
• **Tagged VID**	**Port MEP**: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
• **This MAC**	The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).
• **Alarm**	There is an active alarm on the MEP.

Buttons

Add New MEP: Click to add a new MEP entry

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.19.2 Detailed MEP Configuration

This page allows the user to inspect and configure the current MEP Instance.; screen in Figure 4-19-2 appears.

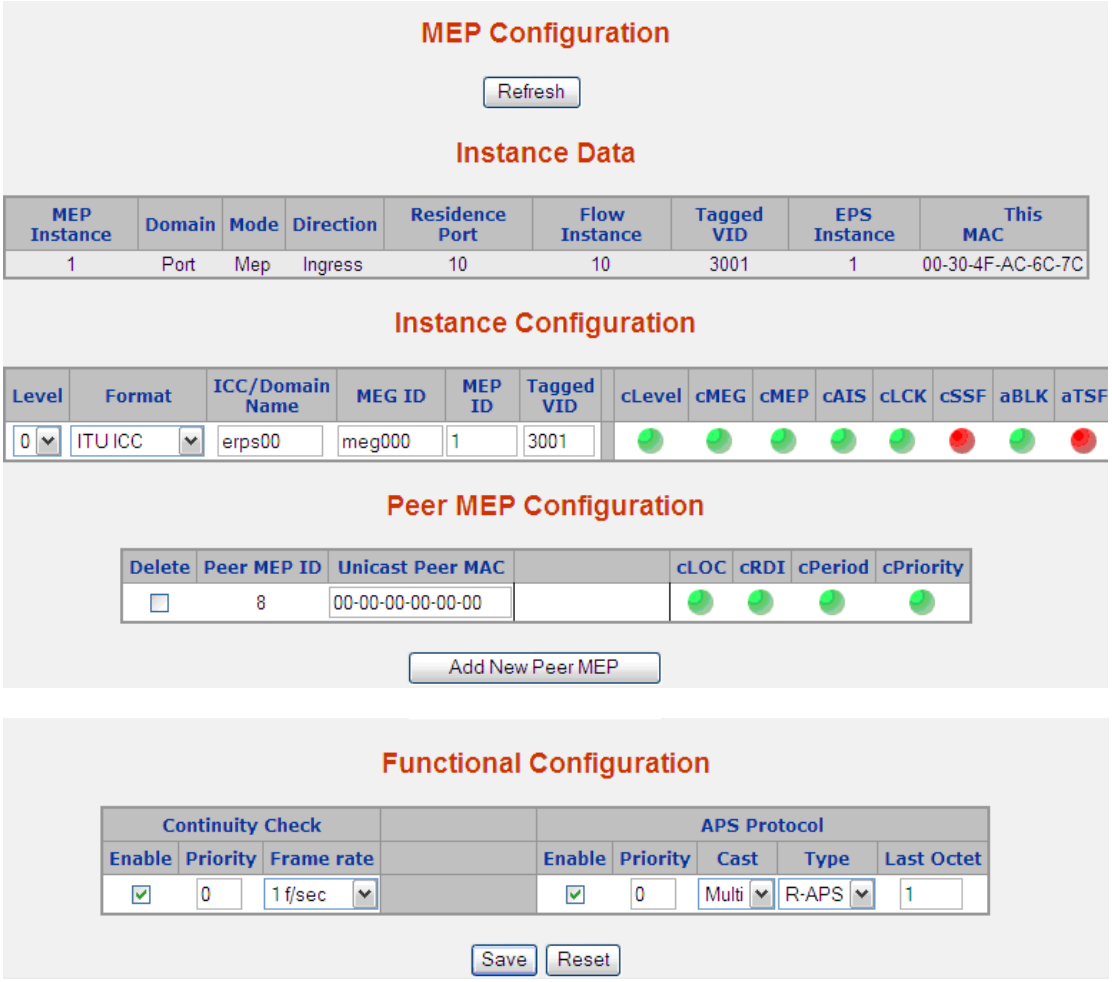


Figure 4-19-2: Detail MEP configuration page screenshot

The page includes the following fields:

Instance Data:

Object	Description
• **MEP Instance**	The ID of the MEP.
• **Domain**	See help on MEP create WEB.
• **Mode**	See help on MEP create WEB.

• **Direction**	See help on MEP create WEB.
• **Residence Port**	See help on MEP create WEB.
• **Flow Instance**	See help on MEP create WEB.
• **Tagged VID**	See help on MEP create WEB.
• **This MAC**	See help on MEP create WEB.

Instance Configuration:

Object	Description
• **Level**	See help on MEP create WEB.
• **Format**	This is the configuration of the two possible Maintenance Association Identifier formats. **ITU ICC**: This is defined by ITU. 'ICC' can be max. 6 char. 'MEG id' can be max. 7 char. **IEEE String**: This is defined by IEEE. 'Domain Name' can be max. 8 char. 'MEG id' can be max. 8 char.
• **ICC/Domain Name**	This is either ITU ICC (MEG ID value [1-6]) or IEEE Maintenance Domain Name - depending on 'Format'. See 'Format'.
• **MEG Id**	This is either ITU UMC (MEG ID value [7-13]) or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this can be max. 7 char. If only 6 char. is entered the MEG ID value [13] will become NULL.
• **MEP Id**	This value will become the transmitted two byte CCM MEP ID.
• **cLevel**	Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.
• **cMEG**	Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.
• **cMEP**	Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.
• **cAIS**	Fault Cause indicating that AIS PDU is received.
• **cLCK**	Fault Cause indicating that LCK PDU is received.
• **cSSF**	Fault Cause indicating that server layer is indicating Signal Fail.
• **aBLK**	The consequent action of blocking service frames in this flow is active.
• **aTSF**	The consequent action of indicating Trail Signal Fail to-wards protection is active.
• **Delete**	This box is used to mark a Peer MEP for deletion in next Save operation.
• **Peer MEP ID**	This value will become an expected MEP ID in a received CCM - see 'cMEP'.
• **Unicast Peer MAC**	This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.
• **cLOC**	Fault Cause indicating that no CCM has been received (in 3.5 periods) - from this peer MEP.
• **cRDI**	Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.
• **cPeriod**	Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

• **cPriority**	Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

Buttons

Add New Peer MEP: Click to add a new peer MEP.

Functional Configuration

Instance Data:

Object	Description
• **Enable**	Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.
• **Priority**	The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.
• **Frame rate**	Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731. This value has the following uses: * The transmission rate of the CCM PDU. * Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'. * Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'. Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

APS Protocol:

Object	Description
• **Enable**	Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.
• **Priority**	The priority to be inserted as PCP bits in TAG (if any).
• **Cast**	Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.
• **Type**	**R-APS**: APS PDU is transmitted as R-APS - this is for ERPS. **L-APS**: APS PDU is transmitted as L-APS - this is for ELPS.
• **Last Octet**	This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

Buttons

Fault Management: Click to go to Fault Management page.

Performance Monitoring: Click to go to Performance Monitor page.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.19.3 Ethernet Ring Protocol Switch

The Ethernet Ring Protection Switch instances are configured here; screen in Figure 4-19-3 appears.

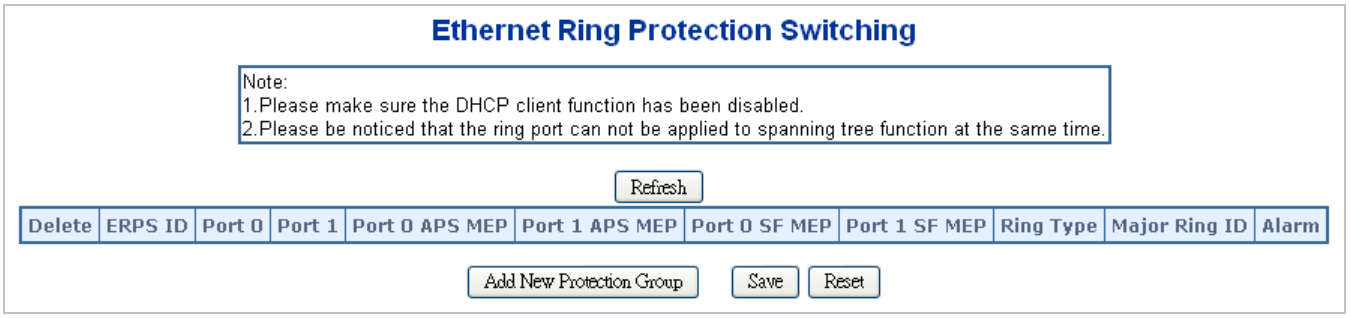


Figure 4-19-3: Ethernet Ring Protocol Switch page screenshot

The page includes the following fields:

Object	Description
• **Delete**	This box is used to mark an ERPS for deletion in next Save operation.
• **Port 0**	This will create a Port 0 of the switch in the ring.
• **Port 1**	This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance
• **Port 0 SF MEP**	The Port 0 Signal Fail reporting MEP.
• **Port 1 SF MEP**	The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 SF MEP is associated with this instance.
• **Port 0 APS MEP**	The Port 0 APS PDU handling MEP.
• **Port 1 APS MEP**	The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.
• **Ring Type**	Type of Protecting ring. It can be either major ring or sub-ring.
• **Major Ring ID**	Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.
• **Alarm**	There is an active alarm on the ERPS.

Buttons

Add New Protection Group: Click to add a new Protection group entry.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.19.4 Ethernet Ring Protocol Switch Configuration

This page allows the user to inspect and configure the current ERPS Instance; screen in Figure 4-19-4 appears.

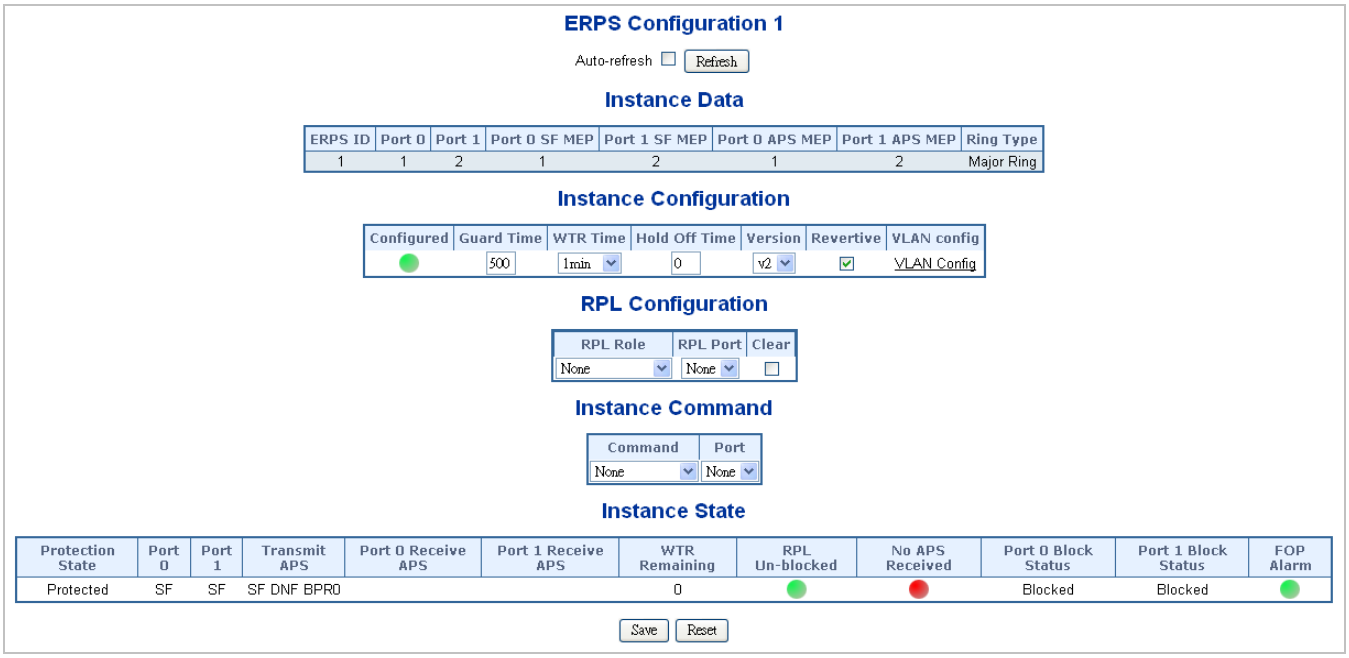


Figure 4-19-4: Ethernet Ring Protocol Switch Configuration page screenshot

The page includes the following fields:

Instance Data:

Object	Description
• **ERPS ID**	The ID of the Protection group.
• **Port 0**	See help on ERPS create WEB.
• **Port 1**	See help on ERPS create WEB.
• **Port 0 SF MEP**	See help on ERPS create WEB.
• **Port 1 SF MEP**	See help on ERPS create WEB.
• **Port 0 APS MEP**	See help on ERPS create WEB.
• **Port 1 APS MEP**	See help on ERPS create WEB.

• **Ring Type**	Type of Protecting ring. It can be either major ring or sub-ring.

Instance Configuration:

Object	Description
• **Configuration**	**Red**: This ERPS is only created and has not yet been configured - is not active. **Green**: This ERPS is configured - is active.
• **Guard Time**	Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds, with a default value of 500 ms
• **WTR Time**	The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.
• **Hold Off Time**	The timing value to be used to make persistent check on Signal Fail before switching. The range of the hold off timer is 0 to 10 seconds in steps of 100 ms
• **Version**	ERPS Protocol Version - v1 or v2
• **Revertive**	In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
• **VLAN Config**	VLAN configuration of the Protection Group. Click on the "VLAN Config" link to confure VLANs for this protection group.

PRL Configuration:

Object	Description
• **PRL Role**	It can be either RPL owner or RPL Neighbour.
• **PRL Port**	This allows to select the east port or west port as the RPL block.
• **Clear**	If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Instance Command:

Object	Description
• **Command**	Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.
• **Port**	Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State:

Object	Description
• **Protection State**	ERPS state according to State Transition Tables in G.8032.

• **Port 0**	**OK**: State of East port is ok **SF**: State of East port is Signal Fail
• **Port 1**	**OK**: State of West port is ok **SF**: State of West port is Signal Fail
• **Transmit APS**	The transmitted APS according to State Transition Tables in G.8032.
• **Port 0 Receive APS**	The received APS on Port 0 according to State Transition Tables in G.8032.
• **Port 1 Receive APS**	The received APS on Port 1 according to State Transition Tables in G.8032.
• **WTR Remaining**	Remaining WTR timeout in milliseconds.
• **RPL Un-blocked**	APS is received on the working flow.
• **No APS Received**	RAPS PDU is not received from the other end.
• **Port 0 Block Status**	Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
• **Port 1 Block Status**	Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.
• **FOP Alarm**	Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows.

Buttons

Save: Click to save changes.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 6 seconds.

Refresh: Click to refresh the page immediately.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.19.5 Ring Wizard

This page allows the user to configure the ERPS by wizard; screen in Figure 4-19-4 appears.

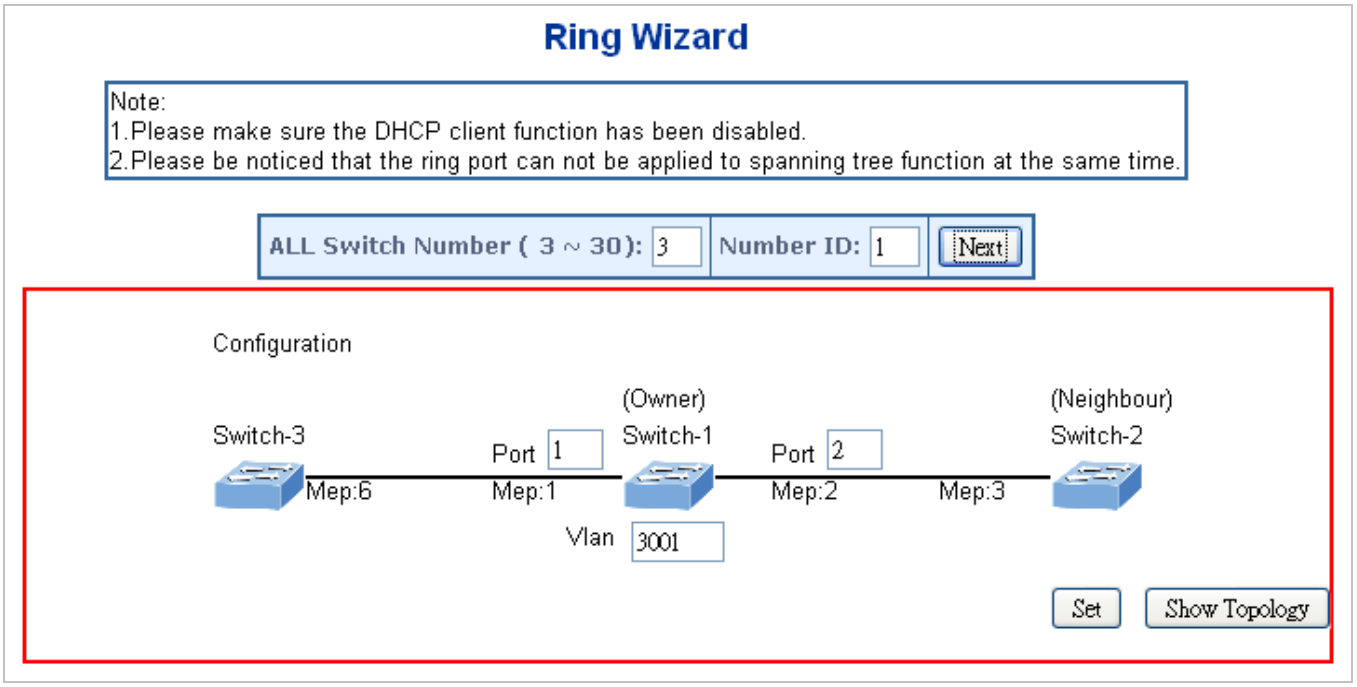


Figure 4-19-5: Ring Wizard page screenshot

The page includes the following fields:

Object	Description
• **All Switch Numbers**	Set all the switch numbers for the ring group. The default number is 3 and maximum number is 30.
• **Number ID**	The switch where you are requesting ERPS.
• **Port**	Configures the port number for the MEP.
• **VLAN**	Set the ERPS VLAN.

Buttons

Next: Click to configure ERPS.

Set: Click to save changes.

Show Topology: Click to show the ring topology.

4.19.6 Ring Wizard Example:

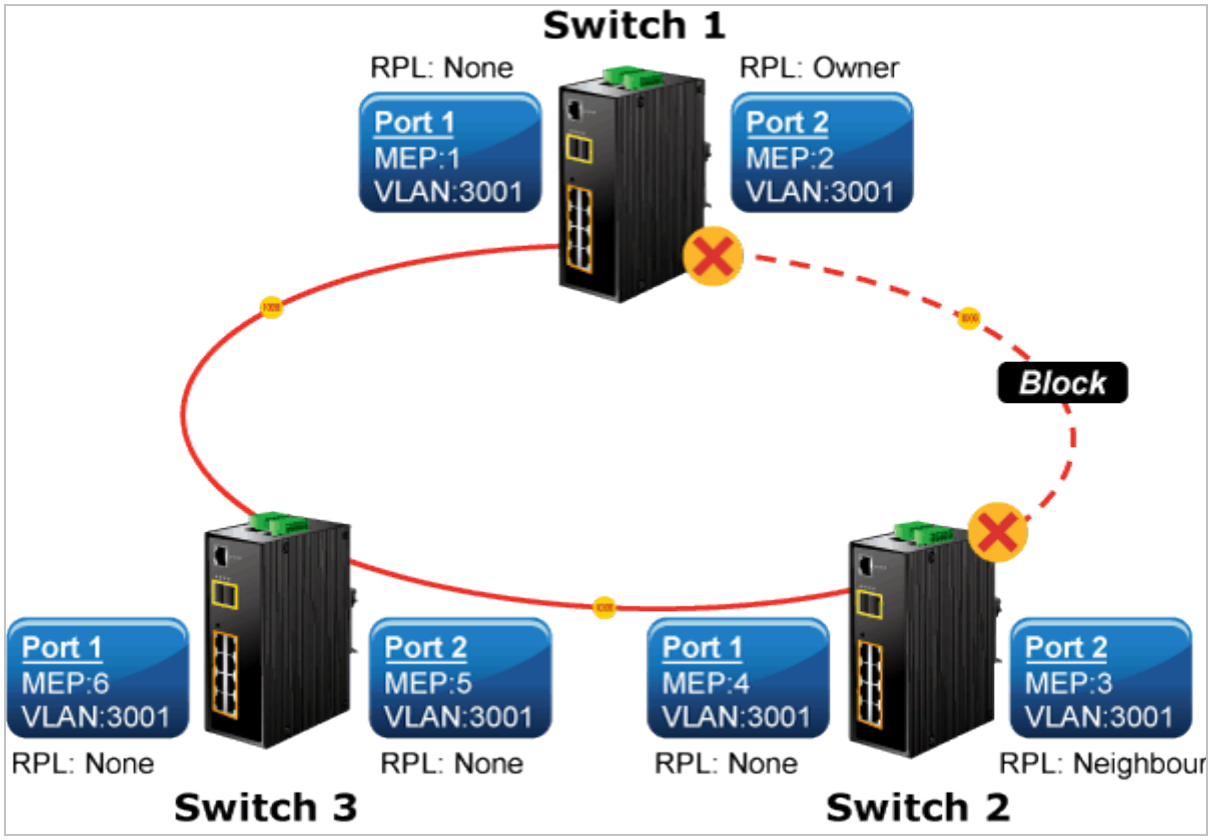


Figure 4-19-6: Ring Example Diagram

The above topology often occurs on using ERPS protocol. The multi switch constitutes a single ERPS ring; all of the switches only are configured as an ERPS in VLAN 3001, thereby constituting a single MRPP ring.

Switch ID	Port	MEP ID	RPL Type	VLAN Group
Switch 1	Port 1	1	None	3001
	Port 2	2	**Owner**	3001
Switch 2	Port 1	4	None	3001
	Port 2	3	**Neighbour**	3001
Switch 3	Port 1	6	None	3001
	Port 2	5	None	3001

Table 4-2: ERPS Configuration Table

The scenario described as follows:

1. Disable DHCP client and set proper static IP for Switch 1, 2 & 3. In this example, switch 1 is 192.168.0.101; switch 2 is 192.168.0.102 and switch 3 is 192.168.0.103.

2. On switch 1, 2 & 3, disable spanning tree protocol to avoid confliction with ERPS.

Setup steps

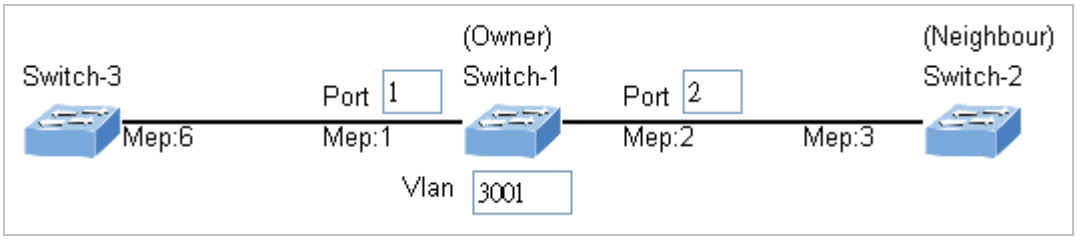
Set ERPS Configuration on Switch 1

Connect PC to switch 1 directly; don't connect to port 1 & 2

Logging on the Switch 1 and click "Ring > Ring Wizard"

Set "All Switch Number" = 3 and "Number ID" = 1; click "Next" button to set the ERPS configuration for Switch 1.

Set "MEP1" = Port1, "MEP2" = Port2 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 1.



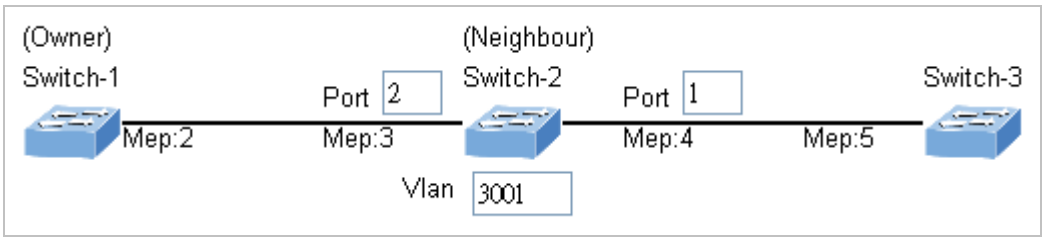
Set ERPS Configuration on Switch 2

Connect PC to switch 2 directly; don't connect to port 1 & 2

Logging on the Switch 2 and click "Ring > Ring Wizard"

Set "All Switch Number" = 3 and "Number ID" = 2; click "Next" button to set the ERPS configuration for Switch 2.

Set "MEP3" = Port2, "MEP4" = Port1 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 2.



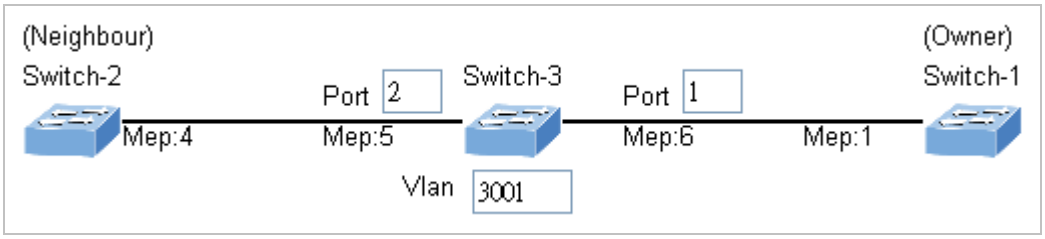
Set ERPS Configuration on Switch 3

Connect PC to switch 3 directly; don't connect to port 1 & 2

Logging on the Switch 3 and click "Ring > Ring Wizard"

Set "All Switch Number" = 3 and "Number ID" = 3; click "Next" button to set the ERPS configuration for Switch 3.

Set "MEP5" = Port2, "MEP6" = Port1 and VLAN ID = 3001; click "Set" button to save the ERPS configuration for Switch 3.



Note

To avoid loop, please don't connect switch 1, 2 & 3 together in the ring topology before configuring the end of ERPS .

Follow the configuration or ERPS wizard to connect the Switch 1, 2 & 3 together to establish ERPS application:

MEP2 ⟷ MEP3 = Switch1 / Port2 ⟷ Switch2 / Port2

MEP4 ⟷ MEP5 = Switch2 / Port1 ⟷ Switch3 / Port2

MEP1 ⟷ MEP6 = Switch1 / Port1 ⟷ Switch3 / Port1

5. COMMAND LINE INTERFACE

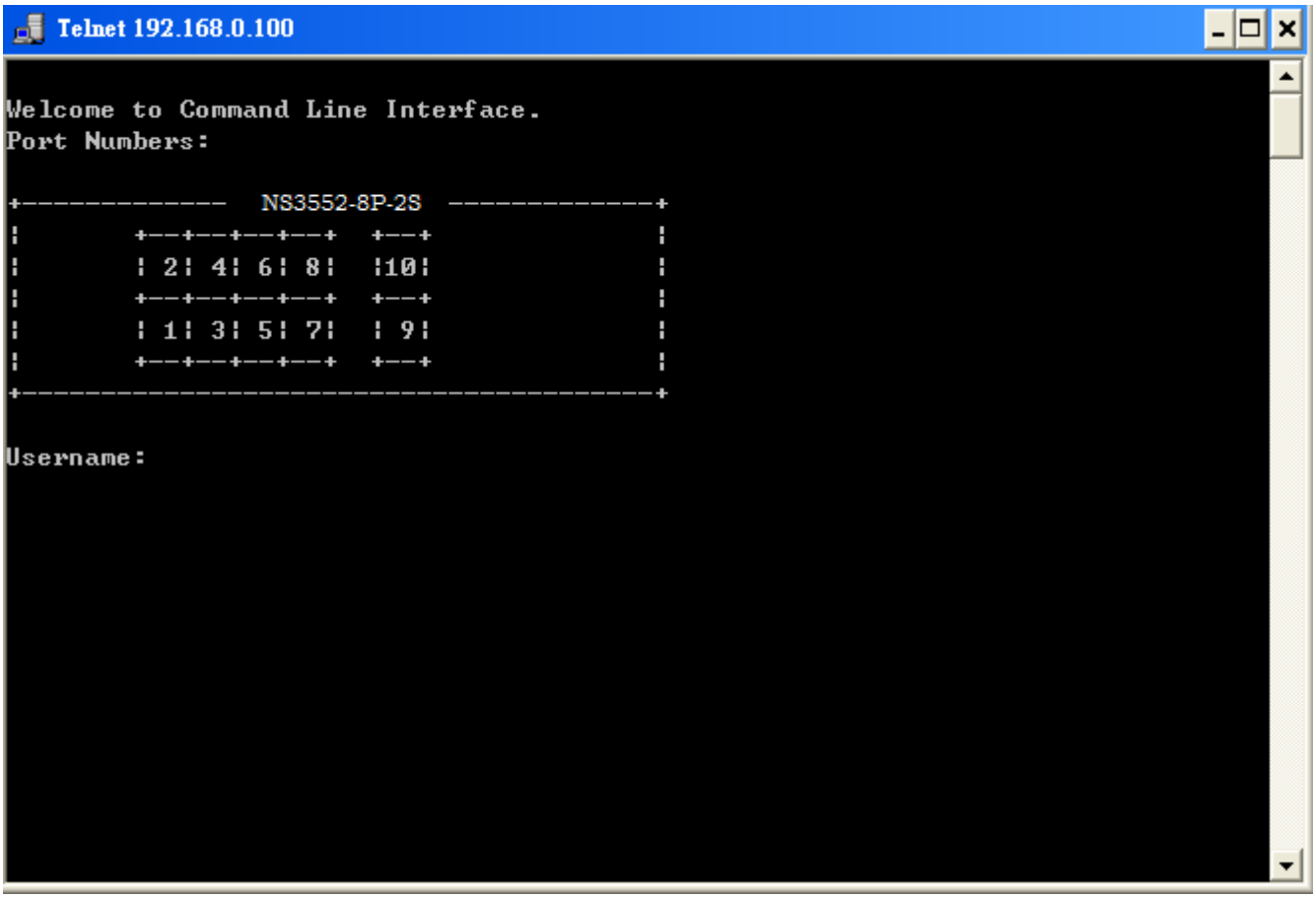
5.1 Accessing the CLI

When accessing the management interface for the **Industrial Managed Switch** via a Telnet connection, the **Industrial Managed Switch** can be managed by entering command keywords and parameters at the prompt. Using the **Industrial Managed Switch**'s command-line interface (CLI) is very similar to entering commands on a UNIX system.

This chapter describes how to use the Command Line Interface (CLI).

5.2 Telnet Login

The **Industrial Managed Switch** supports telnet for remote management. The **Industrial Managed Switch** asks for user name and password for remote login when using telnet, please use **"admin"** for username & password.



6. COMMAND LINE MODE

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes supports specific software commands.

Command Groups:

System	**System settings and reset options**
IP	**IP configuration and Ping**
Port	**Port management**
MAC	**MAC address table**
VLAN	**Virtual LAN**
PVLAN	**Private VLAN**
Security	**Security management**
STP	**Spanning Tree Protocol**
Aggr	**Link Aggregation**
LACP	**Link Aggregation Control Protocol**
LLDP	**Link Layer Discovery Protocol**
LLDPMED	**Link Layer Discovery Protocol Media**
EEE	**Energy Efficient Ethernet**
Thermal	**Thermal Protection**
PoE	**Power Over Ethernet**
EVC	**Ethernet Virtual Connections**
EPS	**Ethernet Protection Switching**
MEP	**Maintainence entity End Point**
QoS	**Quality of Service**
Mirror	**Port mirroring**
Config	**Load/Save of configuration via TFTP**
Firmware	**Download of firmware via TFTP**
UPnP	**Universal Plug and Play**
MVR	**Multicast VLAN Registration**
Voice VLAN	**Specific VLAN for voice traffic**
ERPS	**Ethernet Ring Protection Switching**
Loop Protect	**Loop Protection**
IPMC	**MLD/IGMP Snooping**
VCL	**VLAN Control List**
SMTP	**SMTP Control Configure**
DIDO	**DIDO control configure**
Show	**Show control configuration**

6.1 System Command

System Configuration

Description:

Show system configuration.

Syntax:

System Configuration [all] [<port_list>]

Parameters:

all : Show all switch configuration, default: Show system configuration

port : Show switch port configuration

<port_list>: Port list or 'all', default: All ports

Example:

To display system information:

```
NS3552-8P-2S:/>System configuration
System Contact  :
System Name     : NS3552-8P-2S
System Location :
MAC Address     : 9c-f6-1a-02-7d-70
Temperature     : 27.0 C - 80.6 F
System Time     : 1970-01-01 Thu 03:28:50+00:00
System Uptime   : 03:28:50
Software Version: 1.0b121221
Software Date   : 2012-12-21T14:58:31+0800
Previous Restart: Cold
Power Status    : PWR1 :ON,PWR2 :OFF
NS3552-8P-2S:/>
```

System Log Configuration

Description:

Show system log configuration.

Syntax:

System Log Configuration

Example:

To display system log information:

```
NS3552-8P-2S:/>System log configuration
System Log Configuration:
=========================

System Log Server Mode     : Disabled
System Log Server Address  :
System Log Level           : Info
NS3552-8P-2S:/>
```

System Timezone Configuration

Description:

Show System Timezone configuration.

Syntax:

System Timezone Configuration

System Version

Description:

Show system version information.

Syntax:

System Version

Example:

To display system version:

```
NS3552-8P-2S:/>System version
Version      : 1.0b121221
Build Date   : 2012-12-21T14:58:31+0800
NS3552-8P-2S:/>
```

System Log Server Mode

Description:

Show or set the system log server mode.

Syntax:

System Log Server Mode [enable|disable]

Parameters:

enable : Enable system log server mode

disable: Disable system log server mode

(default: Show system Log server mode)

Default Setting:

disable

Example:

To show the log server mode:

```
NS3552-8P-2S:/>System log server mode
System Log Server Mode     : Disabled
```

System Name

Description:

Set or show the system name.

Syntax:

System Name [<name>]

Parameters:

<name>: System name string. (1-255)

Use "" to clear the string

System name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-).

No blank or space characters are permitted as part of a name.

The first character must be an alpha character, and the first or last character must not be a minus sign.

System Timezone Offset

Description:

Set or show the system timezone offset.

Syntax:

System Timezone Offset [<offset>]

Parameters:

<offset>: Time zone offset in minutes (-7200 to 7201) relative to UTC

System Contact

Description:

Set or show the system contact.

Syntax:

System Contact [<contact>] [clear]

Parameters:

<contact>: System contact string. (1-255)

Use 'clear' or "" to clear the string

In CLI, No blank or space characters are permitted as part of a contact.

clear : Clear system contact

Default Setting:

empty

System Log Server Address

Description:

Show or set the system log server address.

Syntax:

System Log Server Address [<ip_addr_string>]

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Default Setting:

empty

Example:

To set log server address:

```
NS3552-8P-2S:/> log server address 192.168.0.21
```

System Timezone Acronym

Description:

Set or show the system timezone acronym.

Syntax:

System Timezone Acronym [<acronym>]

Parameters:

<acronym>: Time zone acronym (0 - 16 characters)

Default Setting:

empty

System DST Configuration

Description:

Show Daylight Saving Time configuration.

Syntax:

System DST Configuration

System Location

Description:

Set or show the system location.

Syntax:

System Location [<location>]

Parameters:

<location>: System location string. (1-255)

Use 'clear' or "" to clear the string

In CLI, no blank or space characters are permitted as part of a location.

Default Setting:

empty

Example:

To set device location:

```
NS3552-8P-2S:/>System location MyOffice
```

System Log Level

Description:

Show or set the system log level.

It uses to determine what kind of message will send to syslog server.

Syntax:

System Log Level [info|warning|error]

Parameters:

info : Send informations, warnings and errors

warning : Send warnings and errors

error : Send errors

Default Setting:

info

Example:

To set log level:

```
NS3552-8P-2S:/> log level warning
```

System DST Mode

Description:

Set or show the daylight saving time mode.

Syntax:

System DST Mode [disable|recurring|non-recurring]

Parameters:

disable: Disable Daylight Saving Time

recurring : Enable Daylight Saving Time as recurring mode

non-recurring : Enable Daylight Saving Time as non-recurring mode

Default Setting:

Disabled

System DST Start

Description:

Set or show the daylight saving time start time settings.

Syntax:

System DST start <week> <day> <month> <date> <year> <hour> <minute>

Parameters:

<week> : Week (1-5), 0: ignored

<day> : Day (1-7), 0: ignored

<month> : Month (1-12), 0: ignored

<date> : Date (1-31), 0: ignored

<year> : Year (2000-2097)

<hour> : Hour (0-23)

<minute>: Minutes (0-59)

System Log Lookup

Description:

Show the system log.

Syntax:

System Log Lookup [<log_id>] [all|info|warning|error]

Parameters:

<log_id>: System log ID or range (default: All entries)

all : Show all levels (default)

info : Show informations

warning : Show warnings

error : Show errors

System DST End

Description:

end: Set or show the daylight saving time end time settings.

Syntax:

System DST end <week> <day> <month> <date> <year> <hour> <minute>

Parameters:

<week> : Week (1-5), 0: ignored

<day> : Day (1-7), 0: ignored

<month> : Month (1-12), 0: ignored

<date> : Date (1-31), 0: ignored

<year> : Year (2000-2097)

<hour> : Hour (0-23)

<minute>: Minutes (0-59)

System Log Clear

Description:

Clear the system log.

Syntax:

System Log Clear [all|info|warning|error]

Parameters:

all : Show all levels (default)

info : Show informations

warning : Show warnings

error : Show errors

System Reboot

Description:

Reboot the system.

Syntax:

System Reboot

Example:

To reboot device without changing any of the settings:

```
NS3552-8P-2S:/>system reboot
```

System DST Offset

Description:

Set or show the daylight saving time offset.

Syntax:

System DST Offset [<dst_offset>]

Parameters:

<dst_offset>: DST offset in minutes (1 to 1440)

System Restore Default

Description:

Restore factory default configuration.

Syntax:

System Restore Default [keep_ip]

Parameters:

keep_ip: Keep IP configuration, default: Restore full configuration

Example:

To restore default value but not reset IP address:

```
NS3552-8P-2S:/>system restore default keep_ip
```

System Load

Description:

Show current CPU load: 100ms, 1s and 10s running average (in percent, zero is idle).

Syntax:

System Load

Example:

To show current CPU load:

```
NS3552-8P-2S:/>system load
Load average(100ms, 1s, 10s):   1%,   1%,   1%
```

6.2 IP Command

IP Configuration

Description:

Show IP configuration.

Syntax:

IP Configuration

Example:

Show IP configuration:

```
NS3552-8P-2S:/>ip configuration

IP Configuration:
=================

DHCP Client      : Disabled
IP Address       : 192.168.0.101
IP Mask          : 255.255.255.0
IP Router        : 192.168.0.253
DNS Server       : 0.0.0.0
VLAN ID          : 1
DNS Proxy        : Disabled

IPv6 AUTOCONFIG mode   : Disabled
IPv6 Link-Local Address: fe80::6082:cdb9:19ab:c0e2
IPv6 Address          : ::192.168.0.100
IPv6 Prefix           : 96
IPv6 Router           : ::
```

IP DHCP

Description:

Set or show the DHCP client mode.

Syntax:

IP DHCP [enable|disable]

Parameters:

enable : Enable or renew DHCP client

disable: Disable DHCP client

Default Setting:

Disable

Example:

Disable DHCP sever:

```
NS3552-8P-2S:/>ip dhcp disable
```

IP Setup

Description:

Set or show the IP setup.

Syntax:

IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

Parameters:

<ip_addr> : IP address (a.b.c.d), default: Show IP address

<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask

<ip_router>: IP router (a.b.c.d), default: Show IP router

<vid> : VLAN ID (1-4095), default: Show VLAN ID

Default Setting:

IP Address : 192.168.0.100

IP Mask : 255.255.255.0

IP Router : 192.168.0.1

DNS Server : 0.0.0.0

VLAN ID : 1

Example:

Set IP address:

```
NS3552-8P-2S:/>ip setup 192.168.0.100 255.255.255.0
```

IP Ping

Description:

Ping IP address (ICMP echo).

Syntax:

IP Ping <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]

Parameters:

<ip_addr_string>: IPv4 host address (a.b.c.d) or a host name string

length : PING Length keyword

<ping_length> : Ping ICMP data length (2-1452; Default is 56), excluding MAC, IP and ICMP headers

count : PING Count keyword

<ping_count> : Transmit ECHO_REQUEST packet count (1-60; Default is 5)

interval : PING Interval keyword

<ping_interval> : Ping interval (0-30; Default is 0)

IP DNS

Description:

Set or show the DNS server address.

Syntax:

IP DNS [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Showdne IP address

Default Setting:

0.0.0.0

Example:

Set DNS IP address:

```
NS3552-8P-2S:/>ip dns 168.95.1.1
```

IP DNS Proxy

Description:

Set or show the IP DNS Proxy mode.

Syntax:

IP DNS_Proxy [enable|disable]

Parameters:

enable : Enable DNS Proxy

disable: Disable DNS Proxy

Default Setting:

disable

Example:

Enable DNS proxy function:

```
NS3552-8P-2S:/>ip dns_proxy enable
```

IPv6 AUTOCINFIG

Description:

Set or show the IPv6 AUTOCONFIG mode.

Syntax:

IP IPv6 AUTOCONFIG [enable|disable]

Parameters:

enable : Enable IPv6 AUTOCONFIG mode

disable: Disable IPv6 AUTOCONFIG mode

Default Setting:

disable

Example:

Enable IPv6 autoconfig function:

```
NS3552-8P-2S:/>ip ipv6 autoconfig enable
```

IPv6 Setup

Description:

Set or show the IPv6 setup.

Syntax:

IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]

Parameters:

<ipv6_addr> : IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

<ipv6_prefix>: IPv6 subnet mask , default: Show IPv6 prefix

<ipv6_router>: IPv6 router , default: Show IPv6 router. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

Default Setting:

IPv6 AUTOCONFIG mode : Disabled

IPv6 Link-Local Address: fe80::6082:cdb9:19ab:c0e2

IPv6 Address : ::192.168.0.100

IPv6 Prefix : 96

IPv6 Router : ::

Example:

Set IPv6 address:

```
NS3552-8P-2S:/>ip ipv6 setup 2001::0002 64 2100::0001
```

IPv6 State

Description:

Set or show the IPv6 Interface operational state.

Syntax:

IP IPv6 State <ipv6_addr> [enable|disable]

Parameters:

<ipv6_addr>: IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

enable : Enable the designated IPv6 Interface

disable: Disable the designated IPv6 Interface

IPv6 Ping6

Description:

Ping IPv6 address (ICMPv6 echo).

Syntax:

IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]

Parameters:

<ipv6_addr> : IPv6 host address.

IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

length : PING Length keyword

<ping_length> : Ping ICMP data length (2-1452; Default is 56), excluding MAC, IP and ICMP headers

count : PING Count keyword

<ping_count> : Transmit ECHO_REQUEST packet count (1-60; Default is 5)

interval : PING Interval keyword

<ping_interval>: Ping interval (0-30; Default is 0)

IP NTP Configuration

Description:

Show NTP configuration.

Syntax:

IP NTP Configuration

Default Setting:

IP NTP Configuration:

==========

NTP Mode : Disabled

Idx Server IP host address (a.b.c.d) or a host name string

--- ----------

1 pool.ntp.org

2 europe.pool.ntp.org

3 north-america.pool.ntp.org

4 asia.pool.ntp.org

5 oceania.pool.ntp.org

IP NTP Mode

Description:

Set or show the NTP mode.

Syntax:

IP NTP Mode [enable|disable]

Parameters:

enable : Enable NTP mode

disable : Disable NTP mode

(default: Show NTP mode)

Default Setting:

disable

Example:

Enable NTP mode:

```
NS3552-8P-2S:/>ip ntp mode enable
```

IP NTP Server Add

Description:

Add NTP server entry.

Syntax:

IP NTP Server Add <server_index> <ip_addr_string>

Parameters:

<server_index> : The server index (1-5)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Example:

To add NTP server:

```
NS3552-8P-2S:/>ip ntp server add 1 60.249.136.151
```

IP NTP Server IPv6 Add

Description:

Add NTP server IPv6 entry.

Syntax:

IP NTP Server Ipv6 Add <server_index> <server_ipv6>

Parameters:

<server_index>: The server index (1-5)

<server_ipv6> : IPv6 server address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

Example:

To add IPv6 NTP server:

```
NS3552-8P-2S:/>ip ntp server ipv6 add 1 2001:7b8:3:2c::123
```

IP NTP Server Delete

Description:

Delete NTP server entry.

Syntax:

IP NTP Server Delete <server_index>

Parameters:

<server_index>: The server index (1-5)

Example:

To delete NTP server:

```
NS3552-8P-2S:/>ip ntp server delete 1
```

6.3 Port Management Command

Port Configuration

Description:

Show port configuration.

Syntax:

Port Configuration [<port_list>] [up|down]

Parameters:

<port_list>: Port list or 'all', default: All ports

up : Show ports, which are up

down **:** Show ports, which are down

(default: Show all ports)

Example:

Display port1~4 status

```
NS3552-8P-2S:/>port configuration 1-4

Port Configuration:
===================


Port  State    Mode    Flow Control  MaxFrame  Power    Excessive  Link
----  -------- ------  ------------  --------  -------- ---------  ----
1     Enabled  Auto    Disabled      9600      Disabled Discard    Down
2     Enabled  Auto    Disabled      9600      Disabled Discard    Down
3     Enabled  Auto    Disabled      9600      Disabled Discard    Down
4     Enabled  Auto    Disabled      9600      Disabled Discard    Down
```

Port Mode

Description:

Set or show the port speed and duplex mode.

Syntax:

Port Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto : Auto negotiation of speed and duplex

10hdx : 10 Mbps, half duplex

10fdx : 10 Mbps, full duplex

100hdx : 100 Mbps, half duplex

100fdx : 100 Mbps, full duplex

1000fdx : 1 Gbps, full duplex

(default: Show configured and current mode)

Default Setting:

Auto

Example:

Set 10Mbps (half duplex) speed for port1

```
NS3552-8P-2S:/>port mode 1 10hdx
```

Port Flow Control

Description:

Set or show the port flow control mode.

Syntax:

Port Flow Control [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable flow control

disable : Disable flow control

(default: Show flow control mode)

Default Setting:

Disable

Example:

Enable flow control function for port1

```
NS3552-8P-2S:/>port flow control 1 enable
```

Port State

Description:

Set or show the port administrative state.

Syntax:

Port State [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port

disable : Disable port

(default: Show administrative mode)

Default Setting:

Enable

Example:

Disable port1

```
NS3552-8P-2S:/>port state 1 disable
```

Port Maximum Frame

Description:

Set or show the port maximum frame size.

Syntax:

Port MaxFrame [<port_list>] [<max_frame>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<max_frame>: Port maximum frame size (1518-9600), default: Show maximum frame size

Default Setting:

9600

Example:

Set 2048 frame size for port1

```
NS3552-8P-2S:/>port maxframe 1 2048
```

Port Power

Description:

Set or show the port PHY power mode.

Syntax:

Port Power [<port_list>] [enable|disable|actiphy|dynamic]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable all power control

disable: Disable all power control

actiphy: Enable ActiPHY power control

dynamic: Enable Dynamic power control

Default Setting:

disable

Example:

Disable port power function for port1-4

```
NS3552-8P-2S:/>port power 1-4 enable
```

Port Excessive

Description:

Set or show the port excessive collision mode.

Syntax:

Port Excessive [<port_list>] [discard|restart]

Parameters:

<port_list>: Port list or 'all', default: All ports

discard : Discard frame after 16 collisions

restart : Restart backoff algorithm after 16 collisions

(default: Show mode)

Default Setting:

Discard

Example:

```
NS3552-8P-2S:/>port excessive 1 restart
```

Port Statistics

Description:

Show port statistics.

Syntax:

Port Statistics [<port_list>] [<command>] [up|down]

Parameters:

<port_list>: Port list or 'all', default: All ports

<command> : The command parameter takes the following values:

clear : Clear port statistics

packets : Show packet statistics

bytes : Show byte statistics

errors : Show error statistics

discards : Show discard statistics

filtered : Show filtered statistics

0..7 : Show priority statistics

(default: Show all port statistics)

up : Show ports, which are up

down : Show ports, which are down

(default: Show all ports)

Port VeriPHY

Description:

Run cable diagnostics.

Syntax:

Port VeriPHY [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Port SFP

Description:

Show SFP port information.

Syntax:

Port SFP [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show SFP information for port9-10

```
NS3552-8P-2S:/>port sfp

Port  Type           Speed      Wave Length(nm)  Distance(m)
----  -------------    --------     ---------------    -----------
9    1000Base-LX     1000-Base    1310            10000
10    1000Base-LX     1000-Base    1310            10000
```

Port Description

Description:

Set or show Port Description.

Syntax:

Port Description [<port_list>] [<descr_text>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<descr_text>: Text of port description

6.4 MAC Address Table Command

MAC Configuration

Description:

Show MAC address table configuration.

Syntax:

MAC Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show Mac address state

```
NS3552-8P-2S:/>mac configuration

MAC Configuration:
==================

MAC Address    : 9c-f6-1a-03-1c-48
MAC Age Time: 300

Port  Learning
----  --------
1     Auto
2     Auto
3     Auto
4     Auto
5     Auto
6     Auto
7     Auto
8     Auto
9     Auto
10    Auto
```

MAC Add

Description:

Add MAC address table entry.

Syntax:

MAC Add <mac_addr> <port_list> [<vid>]

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

<port_list>: Port list or 'all' or 'none'

<vid> : VLAN ID (1-4095), default: 1

Example:

Add Mac address 00-30-4F-01-01-02 in port1 and vid1

```
NS3552-8P-2S:/>mac add 9c-f6-1a-03-1c-48 1 1
```

MAC Delete

Description:

Delete MAC address entry.

Syntax:

MAC Delete <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095), default: 1

Example:

Delete Mac address 00-30-4F-a1-01-d2 in vid1

```
NS3552-8P-2S:/>mac delete 33-33-4F-a1-01-d2
```

MAC Lookup

Description:

Lookup MAC address entry.

Syntax:

MAC Lookup <mac_addr> [<vid>]

Parameters:

<mac_addr>: MAC address (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095), default: 1

Example:

Lookup state of Mac address **00-30-4F-a1-01-d2**

```
NS3552-8P-2S:/>mac lookup 33-33-4F-a1-01-d2
```

MAC Age Time

Description:

Set or show the MAC address age timer.

Syntax:

MAC Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (0,10-1000000) 0=disable,

(default: Show age time)

Default Setting:

300

Example:

Set agetime value in 30

```
NS3552-8P-2S:/>mac agetime 30
```

MAC Learning

Description:

Set or show the port learn mode.

Syntax:

MAC Learning [<port_list>] [auto|disable|secure]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto : Automatic learning

disable: Disable learning

secure : Secure learning

(default: Show learn mode)

Default Setting:

Auto

Example:

Set secure learning mode in port1

```
NS3552-8P-2S:/>mac learning 1 secure
```

MAC Dump

Description:

Show sorted list of MAC address entries.

Syntax:

MAC Dump [<mac_max>] [<mac_addr>] [<vid>]

Parameters:

<mac_max> : Maximum number of MAC addresses 1-8192, default: Show all addresses

<mac_addr>: First MAC address (xx-xx-xx-xx-xx-xx), default: MAC address zero

<vid> : First VLAN ID (1-4095), default: 1

Example:

Show all of MAC table

```
NS3552-8P-2S:/>mac dump
Type    VID  MAC Address       Ports
------  ---  ----------------  -----
Static  1    00-30-4F-a6-34-9d  None,CPU
Dynamic 1    33-33-4F-a1-01-d2 1
Static  1    33-33-00-00-00-01  1,2,4-10,CPU
Static  1    33-33-00-00-00-02  1,2,4-10,CPU
Static  1    33-33-ff-16-81-68  1,2,4-10,CPU
Static  1    33-33-ff-a8-00-64  1,2,4-10,CPU
Static  1    ff-ff-ff-ff-ff-ff  1-10,CPU
NS3552-8P-2S:/>
```

MAC Statistics

Description:

Show MAC address table statistics.

Syntax:

MAC Statistics [<port_list>]

Parameters:

<port_list>: Port list or 'all',

(default: All ports)

Example:

Set all of MAC statistics

```
NS3552-8P-2S:/>mac statistics
Port  Dynamic Addresses
----  ----------------
1     1
2     0
3     0
4     0
5     0
6     0
7     0
8     0
9     0
10    0

Total Dynamic Addresses: 1
Total Static Addresses : 6
NS3552-8P-2S:/>
```

MAC Flush

Description:

Flush all learned entries.

Syntax:

MAC Flush

6.5 VLAN Configuration Command

VLAN Configuration

Description:

Show VLAN configuration.

Syntax:

VLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all',

(default: All ports)

Example:

Show VLAN status of port1

```
NS3552-8P-2S:/>vlan configuration 1

VLAN Configuration:
====================


Mode : IEEE 802.1Q
Port  PVID  IngrFilter  FrameType   LinkType  Q-in-Q Mode  Eth type
----  ----  ----------  ----------  --------  -----------  --------
1     1     Disabled    All         UnTag     Disable      N/A

VID   VLAN Name                      Ports
----  ---------------------------------  -----
1     default                        1-10

VID   VLAN Name                      Ports
----  ---------------------------------  -----
VLAN forbidden table is empty
```

VLAV PVID

Description:

Set or show the port VLAN ID.

Syntax:

VLAN PVID [<port_list>] [<vid>|none]

Parameters:

<port_list>: Port list or 'all', default: All ports

<vid>|none : Port VLAN ID (1-4095) or 'none',

(default: Show port VLAN ID)

Default Setting:

1

Example:

Set PVID2 for port10

```
NS3552-8P-2S:/>vlan pvid 10 2
```

VLAN Frame Type

Description:

Set or show the port VLAN frame type.

Syntax:

VLAN FrameType [<port_list>] [all|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports

all : Allow tagged and untagged frames

tagged : Allow tagged frames only

(default: Show accepted frame types)

Default Setting:

All

Example:

Set port10 that allow tagged frames only

```
NS3552-8P-2S:/>vlan frametype 10 tagged
```

VLAN Ingress Filter

Description:

Set or show the port VLAN ingress filter.

Syntax:

VLAN IngressFilter [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable VLAN ingress filtering

disable : Disable VLAN ingress filtering

(default: Show VLAN ingress filtering)

Default Setting:

Disable

Example:

Enable VLAN ingress filtering for port10

```
NS3552-8P-2S:/>vlan ingressfilter 10 enable
```

VLAN Mode

Description:

Set or show the VLAN Mode.

Syntax:

VLAN Mode [portbased|dot1q]

Parameters:

portbased : Port-Based VLAN Mode

dot1q : 802.1Q VLAN Mode

(default: Show VLAN Mode)

Default Setting:

IEEE 802.1Q

Example:

Set VLAN mode in port base

```
NS3552-8P-2S:/>vlan mode portbased
```

VLAN Link Type

Description:

Set or show the port VLAN link type.

Syntax:

VLAN LinkType [<port_list>] [untagged|tagged]

Parameters:

<port_list>: Port list or 'all', default: All ports

untagged : VLAN Link Type Tagged

tagged : VLAN Link Type Untagged

(default: Show VLAN link type)

Default Setting:

Un-tagged

Example:

Enable tagged frame for port2

```
NS3552-8P-2S:/>vlan linktype 2 tagged
```

VLAN Q-in-Q Mode

Description:

Set or show the port Q-in-Q mode.

Syntax:

VLAN QinQ [<port_list>] [disable|man|customer]

Parameters:

<port_list>: Port list or 'all', default: All ports

disable : Disable Q-in-Q VLAN Mode

man : Q-in-Q MAN Port Mode

customer : Q-in-Q Customer Port Mode

(default: Show VLAN QinQ Mode)

Example:

Set port2 in man port

```
NS3552-8P-2S:/>vlan qinq 2 man
```

VLAN Ethernet Type

Description:

Set or show out layer VLAN tag ether type in Q-in-Q VLAN mode.

Syntax:

VLAN Ethtype [<port_list>] [man|dot1q]

Parameters:

<port_list>: Port list or 'all', default: All ports

man : Set out layer VLAN tag ether type : MAN

dot1q : Set out layer VLAN tag ether type : 802.1Q

(default: Show VLAN out layer VLAN tag ether type)

Default Setting:

N/A

Example:

Set out layer VLAN tag Ethernet type for port 10 in man Ethernet type

```
NS3552-8P-2S:/>vlan ethtype 10 man
```

VLAN untagVID

Description:

Set or show the port untagVLAN ID.

Syntax:

VLAN untagVID [<port_list>] [<untagvid>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<untagvid> : Port VLAN ID (0-4095) or 'none', default: Show port VLAN ID

If Untag VID = 0 ,then disable untag VID function.

Default Setting:

N/A

VLAN Add

Description:

Add or modify VLAN entry.

Syntax:

VLAN Add <vid>|<name> [<port_list>]

Parameters:

<vid>|<name>: VLAN ID (1-4095) or VLAN Name

<port_list> : Port list or 'all', default: All ports

Default Setting:

1

Example:

Add port1 to port4 in VLAN10

```
NS3552-8P-2S:/>vlan add 10 1-4
```

VLAN Forbidden Add

Description:

Add or modify VLAN entry in forbidden table.

Syntax:

VLAN Forbidden Add <vid>|<name> [<port_list>]

Parameters:

<vid>|<name>: VLAN ID (1-4095) or VLAN Name

<port_list> : Port list or 'all', default: All ports

Example:

Frobidden add port1 to port4 in VLAN10

```
NS3552-8P-2S:/>vlan forbidden add 10 1-4
```

VLAN Delete

Description:

Delete VLAN entry.

Syntax:

VLAN Delete <vid>|<name>

Parameters:

<vid>|<name>: VLAN ID (1-4095) or VLAN Name

Example:

Delete VLAN10

```
NS3552-8P-2S:/>vlan delete 10
```

VLAN Forbidden Delete

Description:

Delete VLAN entry.

Syntax:

LAN Forbidden Delete <vid>|<name>

Parameters:

<vid>|<name>: VLAN ID (1-4095) or VLAN Name

Example:

Forbidden delete VLAN10

```
NS3552-8P-2S:/>vlan forbidden delete 10
```

VLAN Forbidden Lookup

Description:

Lookup VLAN Forbidden port entry.

Syntax:

VLAN Forbidden Lookup [<vid>] [(name <name>)]

Parameters:

<vid> : VLAN ID (1-4095), default: Show all VLANs

name : VLAN name string

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.

VLAN Lookup

Description:

Lookup VLAN entry.

Syntax:

VLAN Lookup [<vid>] [(name <name>)] [combined|static|nas|mvr|voice_vlan|all]

Parameters:

<vid> : VLAN ID (1-4095), default: Show all VLANs

name : VLAN name string

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.

combined : Shows All the Combined VLAN database

static : Shows the VLAN entries configured by the administrator

nas : Shows the VLANs configured by NAS

mvr : Shows the VLANs configured by MVR

voice_vlan : Shows the VLANs configured by Voice VLAN

all : Shows all VLANs configuration

(default: combined VLAN Users configuration)

Example:

Show VLAN status

```
NS3552-8P-2S:/>vlan lookup
```

```
VID   VLAN Name                       Ports
----  --------------------------------  -----
1     default                          1-10
```

VLAN Name Add

Description:

Add VLAN Name to a VLAN ID Mapping.

Syntax:

VLAN Name Add <name> <vid>

Parameters:

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.

<vid> : VLAN ID (1-4095)

Example:

Add VLAN name for VLAN 1

```
NS3552-8P-2S:/>vlan name add test 1
```

VLAN Name Delete

Description:

Delete VLAN Name to VLAN ID Mapping.

Syntax:

VLAN Name Delete <name>

Parameters:

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.

Example:

Delete VLAN name

```
NS3552-8P-2S:/>vlan name delete test
```

VLAN Name Lookup

Description:

Show VLAN Name table.

Syntax:

VLAN Name Lookup [<name>]

Parameters:

<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers.

VLAN name should contain atleast one alphabet.

Example:

To show VLAN Name table

```
NS3552-8P-2S:/>vlan name lookup
VLAN NAME                       vid
------------------------------- ---
test                            1
```

VLAN Status

Description:

VLAN Port Configuration Status.

Syntax:

VLAN Status [<port_list>] [combined|static|nas|mvr|voice_vlan|mstp|all|conflicts]

Parameters:

<port_list>: Port list or 'all', default: All ports

combined : combined VLAN Users configuration

static : static port configuration

nas : NAS port configuration

mvr : MVR port configuration

voice_vlan : Voice VLAN port configuration

mstp : MSTP port configuration

all : All VLAN Users configuration

(default: combined VLAN Users configuration)

Default Setting:

Promiscous

Example:

Show VLAN configuration of port10

```
NS3552-8P-2S:/>status 1

Port  VLAN User    PortType      PVID  Frame Type  Ing Filter   Tx Tag      UVID   Conflicts
----  ----------  ----------  ----  ----------  ----------  -----  ---------
1     Static      Unaware       1     All         Disabled    Untag This  1
      NAS                                                     No
      MVR                                                     No
      Voice VLAN                                                 No
      MSTP                                                    No
      Combined    Unaware       1     All         Disabled    Untag This  1      No
```

6.6 Private VLAN Configuration Command

PVLAN Configuration

Description:

Show Private VLAN configuration.

Syntax:

PVLAN Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show private VLAN configuration

```
NS3552-8P-2S:/> pvlan configuration

Private VLAN Configuration:
===========================


Port  Isolation
----  ---------
1     Disabled
2     Disabled
3     Disabled
4     Disabled
5     Disabled
6     Disabled
7     Disabled
8     Disabled
9     Disabled
10    Disabled

PVLAN ID  Ports
--------  -----
1         1-10
```

PVLAN Add

Description:

Add or modify Private VLAN entry.

Syntax:

PVLAN Add <pvlan_id> [<port_list>]

Parameters:

<pvlan_id> : Private VLAN ID. The allowed range for a Private VLAN ID is the same as the switch port number range.

<port_list>: Port list or 'all', default: All ports

Example:

Add port1 to port4 in PVLAN10

```
NS3552-8P-2S:/>pvlan add 10 1-4
```

PVLAN Delete

Description:

Delete Private VLAN entry.

Syntax:

PVLAN Delete <pvlan_id>

Parameters:

<pvlan_id>: Private VLAN ID. The allowed range for a Private VLAN ID is the same as the switch port number range.

Example:

Delete PVLAN10

```
NS3552-8P-2S:/>pvlan delete 10
```

PVLAN Lookup

Description:

Lookup Private VLAN entry.

Syntax:

PVLAN Lookup [<pvlan_id>]

Parameters:

<pvlan_id>: Private VLAN ID, default: Show all PVLANs. The allowed range for a Private VLAN ID is the same as the switch port number range.

Example:

Lookup PVLAN

```
NS3552-8P-2S:/>pvlan lookup

PVLAN ID  Ports
--------  -----
1         1-10
```

PVLAN Isolate

Description:

Set or show the port isolation mode.

Syntax:

PVLAN Isolate [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port isolation

disable : Disable port isolation

(default: Show port isolation port list)

Default Setting:

disable

Example:

Enable isolate for port10

```
NS3552-8P-2S:/>pvlan isolate 10 enable
```

6.7 Security Command

Security Switch User Configuration

Description:

Show users configuration.

Syntax:

Security Switch Users Configuration

Default Setting:

User Name	Privilege
admin	15

Example:

Show users configuration

```
NS3552-8P-2S:/>security switch user configuration

Users Configuration:
====================

User Name                       Privilege Level
--------------------------------  ----------------
admin                           15
```

Security Switch User Add

Description:

Add or modify users entry.

Syntax:

Security Switch Users Add <user_name> <password> <privilege_level>

Parameters:

<user_name> : A string identifying the user name that this entry should belong to. The allowed string length is (1-32). The valid user name is a combination of letters, numbers and underscores

<password> : The password for this user name. The allowed string length is (0-32). Use 'clear' or "" as null string

<privilege_level>: User privilege level (1-15)

Example:

Add new user: username: test, password: test & privilege: 10

```
NS3552-8P-2S:/>security switch users add test test 10
```

Security Switch User Delete

Description:

Delete users entry.

Syntax:

Security Switch Users Delete <user_name>

Parameters:

<user_name>: A string identifying the user name that this entry should belong to. The allowed string length is (1-32). The valid user name is a combination of letters, numbers and underscores

Example:

Delete test account.

```
NS3552-8P-2S:/>security switch users delete user
```

Security Switch Privilege Level Configuration

Description:

Show privilege configuration.

Syntax:

Security Switch Privilege Level Configuration

Security Switch Privilege Level Group

Description:

Configure a privilege level group.

Syntax:

Security Switch Privilege Level Group <group_name> [<cro>] [<crw>] [<sro>] [<srw>]

Parameters:

<group_name>: Privilege group name

<cro> : Configuration read-only privilege level (1-15)

<crw> : Configuration/Execute read-write privilege level (1-15)

<sro> : Status/Statistics read-only privilege level (1-15)

<srw> : Status/Statistics read-write privilege level (1-15)

Example:

Change privilege level of MVR group.

```
NS3552-8P-2S:/>security switch privilege level group mvr 15 15 15 15
```

Security Switch Privilege Level Current

Description:

Show the current privilege level.

Syntax:

Security Switch Privilege Level Current

Default Setting:

15

Security Switch Auth Configuration

Description:

Show Auth configuration.

Syntax:

Security Switch Auth Configuration

Example:

Show authentication configuration.

```
NS3552-8P-2S:/>security switch auth configuration

Auth Configuration:
==================

Client   Authentication Method   Local Authentication Fallback
-------  ----------------------  ------------------------------
console  local                   Disabled
telnet   local                   Disabled
ssh      local                   Disabled
web      local                   Disabled
```

Security Switch Auth Method

Description:

Set or show Auth method. (default: Show Auth method).

Syntax:

Security Switch Auth Method [console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable]

Parameters:

console : Settings for console

telnet : Settings for telnet

ssh : Settings for ssh

web : Settings for web

(default: Set or show the specific client authentication method)

none : Authentication disabled

local : Use local authentication

radius : Use remote RADIUS authentication

tacacs+ : Use remote TACACS+ authentication

(default: Show client authentication method)

enable : Enable local authentication if remote authentication fails

disable : Disable local authentication if remote authentication fails

(The parameter is effective when it is typed)

Default Setting:

disable

Example:

Use RADIUS authentication method for telnet.

```
NS3552-8P-2S:/>security switch auth method telnet radius enable
```

Security Switch SSH Configuration

Description:

Show SSH configuration.

Syntax:

Security Switch SSH Configuration

Example:

Show SSH configuration.

```
NS3552-8P-2S:/>security switch ssh configuration

SSH Configuration:
==================

SSH Mode : Enable
```

Security Switch SSH Mode

Description:

Set or show the SSH mode.

Syntax:

Security Switch SSH Mode [enable|disable]

Parameters:

enable : Enable SSH

disable: Disable SSH

(default: Show SSH mode)

Default Setting:

enable

Example:

Enable SSH function.

```
NS3552-8P-2S:/>security switch ssh mode enable
```

Security Switch HTTPs Configuration

Description:

Show HTTPS configuration.

Syntax:

Security Switch HTTPS Configuration

Example:

Show HTTPs configuration.

```
NS3552-8P-2S:/>security switch https configuration

HTTPS Configuration:
====================

HTTPS Mode         : Enable
HTTPS Redirect Mode : Disabled
```

Security Switch HTTPs Mode

Description:

Set or show the HTTPS mode.

Syntax:

Security Switch HTTPS Mode [enable|disable]

Parameters:

enable : Enable HTTPs

disable: Disable HTTPs

(default: Show HTTPs mode)

Default Setting:

Enable

Example:

Enable HTTPs function.

```
NS3552-8P-2S:/>security switch https mode enable
```

Security Switch HTTPs Redirect

Description:

Set or show the HTTPS redirect mode.

Automatic redirect web browser to HTTPS during HTTPS mode enabled.

Syntax:

Security Switch HTTPS Redirect [enable|disable]

Parameters:

enable : Enable HTTPs redirect

disable: Disable HTTPs redirect

(default: Show HTTPs redirect mode)

Default Setting:

disable

Example:

Enable HTTPs redirect function.

```
NS3552-8P-2S:/>security switch https redirect enable
```

Security Switch Access Configuration

Description:

Show access management configuration.

Syntax:

Security Switch Access Configuration

Example:

Show access management configuration.

```
NS3552-8P-2S:/>security switch access configuration

Access Mgmt Configuration:
==========================

System Access Mode : Disabled
System Access number of entries: 0
```

Security Switch Access Mode

Description:

Set or show the access management mode.

Syntax:

Security Switch Access Mode [enable|disable]

Parameters:

enable : Enable access management

disable: Disable access management

(default: Show access management mode)

Default Setting:

disable

Example:

Enable access management function.

```
NS3552-8P-2S:/>security switch access mode enable
```

Security Switch Access Add

Description:

Add access management entry, default: Add all supported protocols.

Syntax:

Security Switch Access Add <access_id> <start_ip_addr> <end_ip_addr> [web] [snmp] [telnet]

Parameters:

<access_id> : entry index (1-16)

<start_ip_addr>: Start IP address (a.b.c.d)

<end_ip_addr> : End IP address (a.b.c.d)

web : Indicates that the host can access the switch from HTTP/HTTPS

snmp : Indicates that the host can access the switch from SNMP

telnet : Indicates that the host can access the switch from TELNET/SSH

Example:

Add access management list from 192.168.0.1 to 192.168.0.200 via web interface.

```
NS3552-8P-2S:/>security switch access add 1 192.168.0.1 192.168.0.200 web
```

Security Switch Access IPv6 Add

Description:

Add access management IPv6 entry, default: Add all supported protocols.

Syntax:

Security Switch Access Ipv6 Add <access_id> <start_ipv6_addr> <end_ipv6_addr> [web] [snmp] [telnet]

Parameters:

<access_id> : entry index (1-16)

<start_ipv6_addr>: Start IPv6 address.

IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

<end_ipv6_addr> : End IPv6 address.

IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example,'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

web : Indicates that the host can access the switch from HTTP/HTTPS

snmp : Indicates that the host can access the switch from SNMP

telnet : Indicates that the host can access the switch from TELNET/SSH

Example:

Add access management list from 2001::0001 to 2001::0100 via web interface.

```
NS3552-8P-2S:/> security switch access add 2001::0001 2001::0100 web
```

Security Switch Access Delete

Description:

Delete access management entry.

Syntax:

Security Switch Access Delete <access_id>

Parameters:

<access_id>: entry index (1-16)

Example:

Delete access management ID 1

```
NS3552-8P-2S:/>security switch access delete 1
```

Security Switch Access Lookup

Description:

Lookup access management entry.

Syntax:

Security Switch Access Lookup [<access_id>]

Parameters:

<access_id> : entry index (1-16)

Example:

Lookup access management entry.

```
NS3552-8P-2S:/>security switch access lookup 1
```

Security Switch Access Clear

Description:

Clear access management entry.

Syntax:

Security Switch Access Clear

Example:

Clear access management entry.

```
NS3552-8P-2S:/>security switch access clear
```

Security Switch Access Statistics

Description:

Show or clear access management statistics.

Syntax:

Security Switch Access Statistics [clear]

Parameters:

clear: Clear access management statistics

Example:

Show access management statistics.

```
NS3552-8P-2S:/>security switch access statistics

Access Management Statistics:
------------------------------
HTTP     Receive:         0    Allow:         0    Discard:         0
HTTPS    Receive:         0    Allow:         0    Discard:         0
SNMP     Receive:         0    Allow:         0    Discard:         0
TELNET   Receive:         0    Allow:         0    Discard:         0
SSH      Receive:         0    Allow:         0    Discard:         0
```

Security Switch SNMP Configuration

Description:

Show SNMP configuration.

Syntax:

Security Switch SNMP Configuration

Security Switch SNMP Mode

Description:

Set or show the SNMP mode.

Syntax:

Security Switch SNMP Mode [enable|disable]

Parameters:

enable : Enable SNMP

disable: Disable SNMP

(default: Show SNMP mode)

Default Setting:

enable

Example:

Disable SNMP mode.

```
NS3552-8P-2S:/>security switch snmp mode disable
```

Security Switch SNMP Version

Description:

Set or show the SNMP protocol version.

Syntax:

Security Switch SNMP Version [1|2c|3]

Parameters:

1 : SNMP version 1

2c: SNMP version 2c

3 : SNMP version 3

(default: Show SNMP version)

Default Setting:

2c

Example:

Set SNMP in version 3.

```
NS3552-8P-2S:/>security switch snmp version 3
```

Security Switch SNMP Read Community

Description:

Set or show the community string for SNMP read access.

Syntax:

Security Switch SNMP Read Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string

(default: Show SNMP read community)

Default Setting:

public

Example:

Set SNMP read community private.

```
NS3552-8P-2S:/>security switch snmp read community private
```

Security Switch SNMP Write Community

Description:

Set or show the community string for SNMP write access.

Syntax:

Security Switch SNMP Write Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string

(default: Show SNMP write community)

Default Setting:

private

Example:

Set public value in SNMP write community.

```
NS3552-8P-2S:/>security switch snmp write community public
```

Security Switch SNMP Trap Mode

Description:

Set or show the SNMP trap mode.

Syntax:

Security Switch SNMP Trap Mode [enable|disable]

Parameters:

enable : Enable SNMP traps

disable: Disable SNMP traps

(default: Show SNMP trap mode)

Default Setting:

disable

Example:

Enable SNMP trap mode.

```
NS3552-8P-2S:/>security switch snmp trap mode enable
```

Security Switch SNMP Trap Version

Description:

Set or show the SNMP trap protocol version.

Syntax:

Security Switch SNMP Trap Version [1|2c|3]

Parameters:

1 : SNMP version 1

2c: SNMP version 2c

3 : SNMP version 3

(default: Show SNMP trap version)

Default Setting:

1

Example:

Set SNMP trap version in version 2c.

```
NS3552-8P-2S:/>security switch snmp trap version 2c
```

Security Switch SNMP Trap Community

Description:

Set or show the community string for SNMP traps.

Syntax:

Security Switch SNMP Trap Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string

(default: Show SNMP trap community)

Default Setting:

public

Example:

Set private value for SNMP trap community.

```
NS3552-8P-2S:/>security switch snmp trap community private
```

Security Switch SNMP Trap Destination

Description:

Set or Show the SNMP trap destination address.

Syntax:

Security Switch SNMP Trap Destination [<ip_addr_string>]

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

Example:

Set SNMP trap destination address for 192.168.0.20

```
NS3552-8P-2S:/>security switch snmp trap destination 192.168.0.20
```

Security Switch SNMP Trap IPv6 Destination

Description:

Set or Show the SNMP trap destination IPv6 address.

Syntax:

Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>]

Parameters:

<ipv6_addr>: IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

Example:

Set SNMP trap IPv6 destination address for 2001::0001

```
NS3552-8P-2S:/>security switch snmp trap ipv6 destination 2001::0001
```

Security Switch SNMP Trap Authentication Failure

Description:

Set or show the SNMP authentication failure trap mode.

Syntax:

Security Switch SNMP Trap Authentication Failure [enable|disable]

Parameters:

enable : Enable SNMP trap authentication failure

disable: Disable SNMP trap authentication failure

(default: Show SNMP trap authentication failure mode)

Default Setting:

enable

Example:

Disable SNMP trap authentication failure

```
NS3552-8P-2S:/>security switch snmp trap authentication failure disable
```

Security Switch SNMP Trap Link-up

Description:

Set or show the port link-up and link-down trap mode.

Syntax:

Security Switch SNMP Trap Link-up [enable|disable]

Parameters:

enable : Enable SNMP trap link-up and link-down

disable: Disable SNMP trap link-up and link-down

(default: Show SNMP trap link-up and link-down mode)

Default Setting:

enable

Example:

Disable SNMP trap link-up

```
NS3552-8P-2S:/>security switch snmp trap link-up disable
```

Security Switch SNMP Trap Inform Mode

Description:

Set or show the SNMP trap inform mode.

Syntax:

Security Switch SNMP Trap Inform Mode [enable|disable]

Parameters:

enable : Enable SNMP trap inform

disable: Disable SNMP trap inform

(default: Show SNMP inform mode)

Default Setting:

enable

Example:

Disable SNMP trap inform mode.

```
NS3552-8P-2S:/>security switch snmp trap inform mode disable
```

Security Switch SNMP Trap Inform Timeout

Description:

Set or show the SNMP trap inform timeout (usecs).

Syntax:

Security Switch SNMP Trap Inform Timeout [<timeout>]

Parameters:

<timeout>: SNMP trap inform timeout (0-2147 seconds)

(default: Show SNMP trap inform timeout)

Default Setting:

1

Example:

Set SNMP trap inform timeout in 20sec.

```
NS3552-8P-2S:/>security switch snmp trap inform timeout 20
```

Security Switch SNMP Trap Inform Retry Times

Description:

Set or show the SNMP trap inform retry times.

Syntax:

Security Switch SNMP Trap Inform Retry Times [<retries>]

Parameters:

<retries>: SNMP trap inform retransmited times (0-255)

(default: Show SNMP trap inform retry times)

Default Setting:

5

Example:

Set SNMP trap inform retry times in 10.

```
NS3552-8P-2S:/>security switch snmp trap inform retry times 10
```

Security Switch SNMP Trap Probe Security Engine ID

Description:

Show SNMP trap security engine ID probe mode.

Syntax:

Security Switch SNMP Trap Probe Security Engine ID [enable|disable]

Parameters:

enable : Enable SNMP trap security engine ID probe

disable: Disable SNMP trap security engine ID probe

(default: Show SNMP trap security engine ID probe mode)

Default Setting:

enable

Example:

Disable SNMP trap probe security engine ID

```
NS3552-8P-2S:/>security switch snmp trap probe security engine id disable
```

Security Switch SNMP Trap Security Engine ID

Description:

Set or show SNMP trap security engine ID.

Syntax:

Security Switch SNMP Trap Security Engine ID [<engineid>]

Parameters:

<engineid>: Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

Example:

Set the SNMP trap security engine ID

```
NS3552-8P-2S:/>security switch snmp trap security engine id 800007e5017f000011
```

Security Switch SNMP Trap Security Name

Description:

Set or show SNMP trap security name.

Syntax:

Security Switch SNMP Trap Security Name [<security_name>]

Parameters:

<security_name>: A string representing the security name for a principal (default: Show SNMP trap security name). The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

Example:

Set the SNMP trap security name

```
NS3552-8P-2S:/>security switch snmp trap security name 12345678
```

Security Switch SNMP Engine ID

Description:

Set or show SNMPv3 local engine ID.

Syntax:

Security Switch SNMP Engine ID [<engineid>]

Parameters:

<engineid>: Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

Default Setting:

800007e5017f000001

Example:

Set 800007e5017f000002 for SNMPv3 local engine ID

```
NS3552-8P-2S:/>security switch snmp engine id 800007e5017f000002
```

Security Switch SNMP Community Add

Description:

Add or modify SNMPv3 community entry.

The entry index key is <community>.

Syntax:

Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>]

Parameters:

<community>: Community string

<ip_addr> : IP address (a.b.c.d), default: Show IP address

<ip_mask> : IP subnet mask (a.b.c.d), default: Show IP mask

Example:

Add SNMPv3 community entry.

```
NS3552-8P-2S:/>security switch snmp community add public 192.168.0.20 255.255.255.0
```

Security Switch SNMP Community Delete

Description:

Delete SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 community entry

```
NS3552-8P-2S:/>security switch snmp community delete 3
```

Security Switch SNMP Community Lookup

Description:

Lookup SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 community entry

```
NS3552-8P-2S:/>security switch snmp community lookup
Idx Community                    Source IP       Source Mask
--- ------------------------------          ---------------       ---------------
1   public                       192.168.0.20     255.255.255.0
2   private                       0.0.0.0          0.0.0.0

Number of entries: 2
```

Security Switch SNMP User Add

Description:

Add SNMPv3 user entry.

The entry index key are <engineid> and <user_name> and it doesn't allow modify.

Syntax:

Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]

Parameters:

<engineid> : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

<user_name> : A string identifying the user name that this entry should belong to. The name of "None" is reserved.
The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

md5 : An optional flag to indicate that this user using MD5 authentication protocol. The allowed length is (8-32), and the allowed content is ASCII characters from 33 to 126

sha : An optional flag to indicate that this user using SHA authentication protocol. The allowed length is (8-40), and the allowed content is ASCII characters from 33 to 126

<auth_password>: A string identifying the authentication pass phrase

des : An optional flag to indicate that this user using DES privacy protocol privacy protocol should belong to.
The allowed string length is (8-32), and the allowed content is ASCII characters from 33 to 126

<priv_password>: A string identifying the privacy pass phrase.
The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126

Example:

Add SNMPv3 user entry

```
NS3552-8P-2S:/>security switch snmp user add 800007e5017f000003 admin_snmpv3 md5 12345678 des abcdefgh
```

Security Switch SNMP User Delete

Description:

Delete SNMPv3 user entry.

Syntax:

Security Switch SNMP User Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 user entry

```
NS3552-8P-2S:/>security switch snmp user delete 1
```

Security Switch SNMP User Changekey

Description:

Change SNMPv3 user password.

Syntax:

Security Switch SNMP User Changekey <engineid> <user_name> <auth_password> [<priv_password>]

Parameters:

<engineid> : Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

<user_name> : A string identifying the user name that this entry should belong to. The name of "None" is reserved.
The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

<auth_password>: A string identifying the authentication pass phrase

<priv_password>: A string identifying the privacy pass phrase.
The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126

Example:

Delete SNMPv3 user entry

```
NS3552-8P-2S:/>security switch snmp user changekey 800007e5017f000003 admin_snmpv3
87654321 12345678
```

Security Switch SNMP User Lookup

Description:

Lookup SNMPv3 user entry.

Syntax:

Security Switch SNMP User Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 user entry

```
NS3552-8P-2S:/>security switch snmp user lookup
Idx Engine ID   User Name                       Level         Auth  Priv
--- ---------   --------------------------------            --------------      ----    ----
1   Remote    admin_snmpv3                  Auth, Priv     MD5  DES

Number of entries: 1
```

Security Switch SNMP Group Add

Description:

Add or modify SNMPv3 group entry.

The entry index key are <security_model> and <security_name>.

Syntax:

Security Switch SNMP Group Add <security_model> <security_name> <group_name>

Parameters:

<security_model>: v1 - Reserved for SNMPv1

v2c - Reserved for SNMPv2c

usm - User-based Security Model (USM)

<security_name> : A string identifying the security name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

<group_name> : A string identifying the group name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

Example:

Add SNMPv3 group entry

```
NS3552-8P-2S:/>security switch snmp group add usm admin_snmpv3 group_snmpv3
```

Security Switch SNMP Group Delete

Description:

Delete SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 group entry

```
NS3552-8P-2S:/>security switch snmp group delete 1
```

Security Switch SNMP Group Lookup

Description:

Lookup SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 group entry

```
NS3552-8P-2S:/>security switch snmp group lookup
Idx Model Security Name                  Group Name
--- ----- -------------------------------- --------------------------------
1   v1    public                         default_ro_group
2   v1    private                        default_rw_group
3   v2c   public                         default_ro_group
4   v2c   private                        default_rw_group
5   usm   default_user                       default_rw_group

Number of entries: 5
```

Security Switch SNMP View Add

Description:

Add or modify SNMPv3 view entry.

The entry index key are <view_name> and <oid_subtree>.

Syntax:

Security Switch SNMP View Add <view_name> [included|excluded] <oid_subtree>

Parameters:

<view_name> : A string identifying the view name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

included : An optional flag to indicate that this view subtree should included

excluded : An optional flag to indicate that this view subtree should excluded

<oid_subtree>: The OID defining the root of the subtree to add to the named view

Example:

Add SNMPv3 view entry

```
NS3552-8P-2S:/>security switch snmp view add snmpv3_view include .1
```

Security Switch SNMP View Delete

Description:

Delete SNMPv3 view entry.

Syntax:

Security Switch SNMP View Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 view entry

```
NS3552-8P-2S:/>security switch snmp view delete 3
```

Security Switch SNMP View Lookup

Description:

Lookup SNMPv3 view entry.

Syntax:

Security Switch SNMP View Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 view entry

```
NS3552-8P-2S:/>security switch snmp view lookup
Idx  View Name                       View Type  OID Subtree
---  --------------------------------  ---------  --------------------------------
1   default_view                    included    .1
2   snmpv3_viwe                     included    .1

Number of entries: 2
```

Security Switch SNMP Access Add

Description:

Add or modify SNMPv3 access entry.

The entry index key are <group_name>, <security_model> and <security_level>.

Syntax:

Security Switch SNMP Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]

Parameters:

<group_name> : A string identifying the group name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

<security_model> : any - Accepted any security model (v1|v2c|usm)

v1 - Reserved for SNMPv1

v2c - Reserved for SNMPv2c

usm - User-based Security Model (USM)

<security_level> : noAuthNoPriv - None authentication and none privacy

AuthNoPriv - Authentication and none privacy

AuthPriv - Authentication and privacy

<read_view_name> : The name of the MIB view defining the MIB objects for which this request may request the current values.

The name of "None" is reserved.

The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

<write_view_name>: The name of the MIB view defining the MIB objects for which this request may potentially SET new values.

The name of "None" is reserved.

The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

Example:

Add SNMPv3 access entry

```
NS3552-8P-2S:/>security switch snmp access add group_snmpv3 usm authpriv
snmpv3_view snmpv3_view
```

Security Switch SNMP Access Delete

Description:

Delete SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Delete <index>

Parameters:

<index>: entry index (1-64)

Example:

Delete SNMPv3 access entry

```
NS3552-8P-2S:/>security switch snmp access delete 3
```

Security Switch SNMP Access Lookup

Description:

Lookup SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Lookup [<index>]

Parameters:

<index>: entry index (1-64)

Example:

Lookup SNMPv3 access entry

```
NS3552-8P-2S:/>security switch snmp access lookup
Idx Group Name                    Model Level
--- ------------------------------- ----- --------------
1   default_ro_group               any   NoAuth, NoPriv
2   default_rw_group               any   NoAuth, NoPriv

Number of entries: 2
```

Security Switch RMON Statistics Add

Description:

Add or modify RMON Statistics entry. The entry index key is <stats_id>.

Syntax:

Security Switch RMON Statistics Add <stats_id> <data_source>

Parameters:

<stats_id> : Statistics ID (1-65535).

<data_source>: The OID that indicates that the ifIndex in ifEntry.

The value should be like .1.3.6.1.2.1.2.2.1.1.xxx.

Security Switch RMON Statistics Delete

Description:

Delete RMON Statistics entry. The entry index key is <stats_id>.

Syntax:

Security Switch RMON Statistics Delete <stats_id>

Parameters:

<stats_id>: Statistics ID (1-65535).

Security Switch RMON Statistics Lookup

Description:

Show RMON Statistics entries.

Syntax:

Security Switch RMON Statistics Lookup [<stats_id>]

Parameters:

<stats_id>: Statistics ID (1-65535).

Security Switch RMON History Add

Description:

Add or modify RMON Hisotry entry. The entry index key is <history_id>.

Syntax:

Security Switch RMON History Add <history_id> <data_source> [<interval>] [<buckets>]

Parameters:

<history_id> : History ID (1-65535).

<data_source>: The OID that indicates that the ifIndex in ifEntry.

The value should be like .1.3.6.1.2.1.2.2.1.1.xxx.

<interval> : Sampling interval (1-3600) (default: 1800).

<buckets> : The maximum data entries associated this History control entry stored in RMON(1-65535) (default: 50).

Security Switch RMON History Delete

Description:

Delete RMON Hisotry entry. The entry index key is <history_id>.

Syntax:

Security Switch RMON History Delete <history_id>

Parameters:

<history_id> : History ID (1-65535).

Security Switch RMON History Lookup

Description:

Show RMON History entries.

Syntax:

Security Switch RMON History Lookup [<history_id>]

Parameters:

<history_id> : History ID (1-65535).

Security Switch RMON Alarm Add

Description:

Add or modify RMON Alarm entry. The entry index key is <alarm_id>.

Syntax:

Security Switch RMON Alarm Add <alarm_id> <interval> <alarm_vairable> [absolute|delta] <rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index> [rising|falling|both]

Parameters:

<alarm_id> : Alarm ID (1-65535).

<interval> : Sampling interval (1-2147483647) (default: 30).

<alarm_vairable> : The MIB OID that need to be referenced.

.1.3.6.1.2.1.2.2.1.10.xxx – ifInOctets

.1.3.6.1.2.1.2.2.1.11.xxx – ifInUcastPkts

.1.3.6.1.2.1.2.2.1.12.xxx – ifInNUcastPkts

.1.3.6.1.2.1.2.2.1.13.xxx – ifInDiscards

.1.3.6.1.2.1.2.2.1.14.xxx – ifInErrors

.1.3.6.1.2.1.2.2.1.15.xxx – ifInUnkownProtos

.1.3.6.1.2.1.2.2.1.16.xxx – ifOutOctets

.1.3.6.1.2.1.2.2.1.17.xxx – ifOutUcastPkts

.1.3.6.1.2.1.2.2.1.18.xxx – ifOutNUcastPkts

.1.3.6.1.2.1.2.2.1.19.xxx – ifOutDiscards

.1.3.6.1.2.1.2.2.1.20.xxx – ifOutErrors

.1.3.6.1.2.1.2.2.1.21.xxx – ifOutQLen

"xxx" means the interface identified by a particular value of this index is the same interface as identified by the same value of OID 'ifIndex'.

absolute : Get the sample directly.

delta : Calculate the difference between samples (default).

<rising_threshold> : Rising threshold value (-2147483648–2147483647).

<rising_event_index> : Rising event index (1-65535).

<falling_threshold> : Falling threshold value (-2147483648–2147483647).

<falling_event_index>: Falling event index (1-65535).

rising : Trigger alarm when the first value is larger than the rising threshold.

falling : Trigger alarm when the first value is less than the falling threshold.

both : Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)

Security Switch RMON Alarm Delete

Description:

Delete RMON Alarm entry. The entry index key is <alarm_id>.

Syntax:

Security Switch RMON Alarm Delete <alarm_id>

Parameters:

<alarm_id>: Alarm ID (1-65535).

Security Switch RMON Alarm Lookup

Description:

Show RMON Alarm entries.

Syntax:

Security Switch RMON Alarm Lookup [<alarm_id>]

Parameters:

<alarm_id>: Alarm ID (1-65535).

Security Switch RMON Event Add

Description:

Add or modify RMON Event entry. The entry index key is <event_id>.

Syntax:

Security Switch RMON Event Add <event_id> [none|log|trap|log_trap] [<community>] [<description>]

Parameters:

<event_id> : Event ID (1-65535).

none : Get the sample directly.

log : Get the sample directly.

trap : Get the sample directly.

log_trap : Calculate the difference between samples (default).

<community> : Specify the community when trap is sent (the string lengh is 0~127) (default: public).

<description>: The string for describing this event (the string lengh is 0~127) (default: null string).

Security Switch RMON Event Delete

Description:

Delete RMON Event entry. The entry index key is <event_id>.

Syntax:

Security Switch RMON Event Delete <event_id>

Parameters:

<event_id> : Event ID (1-65535).

Security Switch RMON Event Lookup

Description:

Show RMON Event entries.

Syntax:

Security Switch RMON Event Lookup [<event_id>]

Parameters:

<event_id> : Event ID (1-65535).

Security Network Psec Switch

Description:

Show Port Security status.

Syntax:

Security Network Psec Switch [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show port security status.

```
NS3552-8P-2S:/>security network psec switch
Users:
L = Limit Control
8 = 802.1X
D = DHCP Snooping
V = Voice VLAN

Port  Users  State          MAC Cnt
----  -----  -------------  -------
1     ----   No users       0
2     ----   No users       0
3     ----   No users       0
4     ----   No users       0
5     ----   No users       0
6     ----   No users       0
7     ----   No users       0
8     ----   No users       0
9     ----   No users       0
10    ----   No users       0
```

Security Network Psec Port

Description:

Show MAC Addresses learned by Port Security.

Syntax:

Security Network Psec Port [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show MAC address learned on port 1

```
NS3552-8P-2S:/>security network psec port 1

Port 1:
-------

MAC Address       VID  State      Added                    Age/Hold Time
-----------------  ----  ----------  -------------------------  -------------
<none>
```

Security Network Limit Configuration

Description:

Show Limit Control configuration.

Syntax:

Security Network Limit Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show Limit Control configuration.

```
NS3552-8P-2S:/>security network limit configuration

Port Security Limit Control Configuration:
==========================================

Mode     : Disabled
Aging    : Disabled
Age Period: 3600

Port  Mode      Limit  Action
----  --------  -----  ---------------
1     Disabled     4   None
```

```
2    Disabled     4   None
3    Disabled     4   None
4    Disabled     4   None
5    Disabled     4   None
6    Disabled     4   None
7    Disabled     4   None
8    Disabled     4   None
9    Disabled     4   None
10   Disabled     4   None
```

Security Network Limit Mode

Description:

Set or show global enabledness.

Syntax:

Security Network Limit Mode [enable|disable]

Parameters:

enable : Globally enable port security

disable : Globally disable port security

(default: Show current global enabledness of port security limit control)

Default Setting:

disable

Example:

Enable the limit mode

```
NS3552-8P-2S:/>security network limit mode enable
```

Security Network Limit Aging

Description:

Set or show aging enabledness.

Syntax:

Security Network Limit Aging [enable|disable]

Parameters:

enable : Enable aging

disable : Disable aging

(default: Show current enabledness of aging)

Default Setting:

disable

Example:

Enable limit aging

```
NS3552-8P-2S:/>security network limit aging enable
```

Security Network Limit Agetime

Description:

Time in seconds between check for activity on learned MAC addresses.

Syntax:

Security Network Limit Agetime [<age_time>]

Parameters:

<age_time>: Time in seconds between checks for activity on a MAC address (10-10000000 seconds)

(default: Show current age time)

Default Setting:

3600

Example:

Set age time in 100sec.

```
NS3552-8P-2S:/>security network limit agetime 100
```

Security Network Limit Port

Description:

Set or show per-port enabledness.

Syntax:

Security Network Limit Port [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port security on this port

disable : Disable port security on this port

(default: Show current port enabledness of port security limit control)

Default Setting:

disable

Example:

Enable port limit for port 1

```
NS3552-8P-2S:/>security network limit port 1 enable
```

Security Network Limit Limit

Description:

Set or show the max. number of MAC addresses that can be learned on this set of ports.

Syntax:

Security Network Limit Limit [<port_list>] [<limit>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<limit> : Max. number of MAC addresses on this port

(default: Show current limit)

Default Setting:

4

Example:

Set limit in 5

```
NS3552-8P-2S:/>security network limit limit 1-10 5
```

Security Network Limit Action

Description:

Set or show the action involved with exceeding the limit.

Syntax:

Security Network Limit Action [<port_list>] [none|trap|shut|trap_shut]

Parameters:

<port_list> : Port list or 'all', default: All ports

none|trap|shut|trap_shut: Action to be taken in case the number of MAC addresses exceeds the limit

none : Don't do anything

trap : Send an SNMP trap

shut : Shutdown the port

trap_shut: Send an SNMP trap and shutdown the port

(default: Show current action)

Default Setting:

none

Example:

Set trap mode for limit action for port 1

```
NS3552-8P-2S:/>security network limit action 1 trap
```

Security Network Limit Reopen

Description:

Reopen one or more ports whose limit is exceeded and shut down.

Syntax:

Security Network Limit Reopen [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Reopen port 1

```
NS3552-8P-2S:/>security network limit reopen 1
```

Security Network NAS Configuration

Description:

Show 802.1X configuration.

Syntax:

Security Network NAS Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show 802.1X configuration of port 1

```
NS3552-8P-2S:/>security network nas configuration 1

802.1X Configuration:
=====================

Mode            : Disabled
Reauth.         : Disabled
Reauth. Period  : 3600
EAPOL Timeout   : 30
Age Period      : 300
Hold Time       : 10
RADIUS QoS      : Disabled
RADIUS VLAN     : Disabled
Guest VLAN      : Disabled
Guest VLAN ID   : 1
Max. Reauth Count: 2
Allow Guest VLAN if EAPOL Frame Seen: Disabled

Port  Admin State        Port State           Last Source       Last ID
----  -----------------  -------------------  ----------------  ----------
1     Force Authorized   Globally Disabled     -                 -
```

Security Network NAS Mode

Description:

Set or show the global NAS enabledness.

Syntax:

Security Network NAS Mode [enable|disable]

Parameters:

enable : Globally enable 802.1X

disable: Globally disable 802.1X

(default: Show current 802.1X global enabledness)

Default Setting:

disable

Example:

Enable IEEE802.1X function

```
NS3552-8P-2S:/>security network nas mode enable
```

Security Network NAS State

Description:

Set or show the port security state.

Syntax:

Security Network NAS State [<port_list>] [auto|authorized|unauthorized|single|multi|macbased]

Parameters:

<port_list>: Port list or 'all', default: All ports

auto : Port-based 802.1X Authentication

authorized : Port access is allowed

unauthorized: Port access is not allowed

single : Single Host 802.1X Authentication

multi : Multiple Host 802.1X Authentication

macbased : Switch authenticates on behalf of the client

(default: Show 802.1X state)

Default Setting:

none

Example:

Show the port 1 security state.

```
NS3552-8P-2S:/>security network nas state 1

Port  Admin State        Port State           Last Source       Last ID
----  -----------------  -------------------  ----------------  -----------------
1     Force Authorized   Globally Disabled    -                 -
```

Security Network NAS Reauthentication

Description:

Set or show Reauthentication enabledness.

Syntax:

Security Network NAS Reauthentication [enable|disable]

Parameters:

enable : Enable reauthentication

disable: Disable reauthentication

(default: Show current reauthentication mode)

Default Setting:

disable

Example:

Enable reauthentication function.

```
NS3552-8P-2S:/>security network nas reauthentication enable
```

Security Network NAS ReauthPeriod

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned VLAN.

Syntax:

Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned VLAN setting

<port_list>: Select the per-port RADIUS-assigned VLAN setting

(default: Show current per-port RADIUS-assigned VLAN enabledness)

enable : Enable RADIUS-assigned VLAN either globally or on one or more ports

disable: Disable RADIUS-assigned VLAN either globally or on one or more ports

(default: Show current RADIUS-assigned VLAN enabledness)

Default Setting:

disable

Example:

Enable RADIUS-assigned VLAN.

```
NS3552-8P-2S:/>security network nas radius_vlan enable
```

Security Network NAS EapolTimeout

Description:

Set or show the time between EAPOL retransmissions.

Syntax:

Security Network NAS EapolTimeout [<eapol_timeout>]

Parameters:

<eapol_timeout>: Time between EAPOL retransmissions (1-65535 seconds)

(default: Show current EAPOL retransmission timeout)

Default Setting:

30

Example:

Set the time between EAPOL retransmissions for 100sec.

```
NS3552-8P-2S:/>security network nas eapoltimeout 100
```

Security Network NAS Agetime

Description:

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

Security Network NAS Agetime [<age_time>]

Parameters:

<age_time>: Time between checks for activitiy on a MAC address that succeeded autentication

(default: Show current age time)

Default Setting:

300

Example:

Set NAS age time in 1000sec

```
NS3552-8P-2S:/>security network nas agetime 1000
```

Security Network NAS Holdtime

Description:

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

Security Network NAS Holdtime [<hold_time>]

Parameters:

<hold_time>: Hold time before MAC addresses that failed authentication expire

(default: Show current hold time)

Default Setting:

10

Example:

Set NAS hold time in 100sec

```
NS3552-8P-2S:/>security network nas holdtime 100
```

Security Network NAS RADIUS_QoS

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned QoS.

Syntax:

Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned QoS setting

<port_list>: Select the per-port RADIUS-assigned QoS setting

(default: Show current per-port RADIUS-assigned QoS enabledness)

enable : Enable RADIUS-assigned QoS either globally or on one or more ports

disable: Disable RADIUS-assigned QoS either globally or on one or more ports

(default: Show current RADIUS-assigned QoS enabledness)

Default Setting:

disable

Example:

Enable NAS RADIUS QoS

```
NS3552-8P-2S:/>security network nas radius_qos enable
```

Security Network NAS RADIUS_VLAN

Description:

Set or show either global enabledness (use the global keyword) or per-port enabledness of RADIUS-assigned VLAN.

Syntax:

Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned VLAN setting

<port_list>: Select the per-port RADIUS-assigned VLAN setting

(default: Show current per-port RADIUS-assigned VLAN enabledness)

enable : Enable RADIUS-assigned VLAN either globally or on one or more ports

disable: Disable RADIUS-assigned VLAN either globally or on one or more ports

(default: Show current RADIUS-assigned VLAN enabledness)

Default Setting:

disable

Example:

Enable NAS RADIUS VLAN

```
NS3552-8P-2S:/>security network nas radius_vlan enable
```

Security Network NAS Guest_VLAN

Description:

Set or show either global enabledness and parameters (use the global keyword) or per-port enabledness of Guest VLAN

Unless the 'global' keyword is used, the <reauth_max> and <allow_if_eapol_seen> parameters will not be unused..

Syntax:

Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>]

Parameters:

global: Select the global Guest VLAN setting

<port_list>: Select the per-port Guest VLAN setting

(default: Show current per-port Guest VLAN enabledness)

enable|disable: enable : Enable Guest VLAN either globally or on one or more ports

disable: Disable Guest VLAN either globally or on one or more ports

(default: Show current Guest VLAN enabledness)

<vid>: Guest VLAN ID used when entering the Guest VLAN. Use the 'global' keyword to change it

(default: Show current Guest VLAN ID)

<reauth_max>: The value can only be set if you use the 'global' keyword in the beginning of the command. The number of times a Request Identity EAPOL frame is sent without reasponse before considering entering the Guest VLAN

(default: Show current Maximum Reauth Count value)

<allow_if_eapol_seen>: The value can only be set if you use the 'global' keyword in the beginning of the command.

disable:The Guest VLAN can only be entered if no EAPOL frames have been received on a port for the lifetime of the port

enable :The Guest VLAN can be entered even if an EAPOL frame has been received during the lifetime of the port

(default: Show current setting)

Default Setting:

Disable

Example:

Enable NAS guest VLAN

```
NS3552-8P-2S:/>security network nas guest_vlan enable
```

Security Network NAS Authenticate

Description:

Refresh (restart) 802.1X authentication process.

Syntax:

Security Network NAS Authenticate [<port_list>] [now]

Parameters:

<port_list>: Port list or 'all', default: All ports

now: Force reauthentication immediately

Example:

Start NAS authentication now for port 1.

```
NS3552-8P-2S:/>security network nas authenticate 1 now
```

Security Network NAS Statistics

Description:

Show or clear 802.1X statistics.

Syntax:

Security Network NAS Statistics [<port_list>] [clear|eapol|radius]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear statistics

eapol : Show EAPOL statistics

radius : Show Backend Server statistics

(default: Show all statistics)

Example:

Show 802.1X statistics in port 1

```
NS3552-8P-2S:/>security network nas statistics 1
Port 1 EAPOL Statistics:

Rx Total:                0   Tx Total:                0
Rx Response/Id:          0   Tx Request/Id:           0
Rx Response:             0   Tx Request:              0
Rx Start:                0
Rx Logoff:               0
Rx Invalid Type:         0
Rx Invalid Length:       0

Port 1 Backend Server Statistics:

Rx Access Challenges:    0   Tx Responses:            0
Rx Other Requests:       0
Rx Auth. Successes:      0
Rx Auth. Failures:       0
```

Security Network ACL Configuration

Description:

Show ACL Configuration.

Syntax:

Security Network ACL Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Security Network ACL Action

Description:

Set or show the ACL port default action.

Syntax:

Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]

Parameters:

<port_list> : Port list or 'all', default: All ports

permit : Permit forwarding (default)

deny : Deny forwarding

<rate_limiter>: Rate limiter number (1-15) or 'disable'

<port_copy> : Port number for copy of frames or 'disable'

<logging> : System logging of frames: log|log_disable

<shutdown> : Shut down ingress port: shut|shut_disable

Example:

Show ACL action in port 1

```
NS3552-8P-2S:/>security network acl action 1

Port  Action  Rate Limiter  Port Copy  Mirror   Logging   Shutdown  Counter
----  ------  ------------  ---------  --------  --------  --------  -------
1     Permit  Disabled      Disabled   Disabled  Disabled  Disabled  0
```

Security Network ACL Policy

Description:

Set or show the ACL port policy.

Syntax:

Security Network ACL Policy [<port_list>] [<policy>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<policy> : Policy number (1-8)

Default Setting:

1

Example:

Set ACL policy 2 for port 1

```
NS3552-8P-2S:/>security network acl policy 1 2
```

Security Network ACL Rate

Description:

Set or show the ACL rate limiter.

Syntax:

Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]

Parameters:

<rate_limiter_list>: Rate limiter list (1-16), default: All rate limiters

<rate_unit> : IP flags: pps|kbps, default: pss

<rate> : Rate in pps (0-100) or kbps (0, 100, 2*100, 3*100, ..., 1000000)

Default Setting:

1

Example:

Set rate limit value in 100 for port 1

```
NS3552-8P-2S:/>security network acl rate 1 100
```

Security Network ACL Add

Description:

Add or modify Access Control Entry (ACE).

If the ACE ID parameter <ace_id> is specified and an entry with this ACE ID already exists, the ACE will be modified. Otherwise, a new ACE will be added. If the ACE ID is not specified, the next available ACE ID will be used.

If the next ACE ID parameter <ace_id_next> is specified, the ACE will be placed before this ACE in the list. If the next ACE ID is not specified, the ACE will be placed last in the list.

If the Switch keyword is used, the rule applies to all ports.

If the Port keyword is used, the rule applies to the specified port only. If the Policy keyword is used, the rule applies to all ports configured with the specified policy. The default is that the rule applies to all ports.

Syntax:

Security Network ACL Add [<ace_id>] [<ace_id_next>] [switch | (port <port_list>) | (policy <policy>)] [<tagged>] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>]

[<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_copy>] [<mirror>] [<logging>] [<shutdown>]

Parameters:

<ace_id> : ACE ID (1-256), default: Next available ID

<ace_id_next> : Next ACE ID (1-256), default: Add ACE last

switch : Switch ACE keyword

port : Port ACE keyword

<port_list> : Port list or 'all', default: All ports

policy : Policy ACE keyword

<policy> : Policy number (1-8)

<tagged> : Tagged of frames: any|enable|disable

<vid> : VLAN ID (1-4095) or 'any'

<tag_prio> : VLAN tag priority (0-7) or 'any'

<dmac_type> : DMAC type: any|unicast|multicast|broadcast

etype : Ethernet Type keyword

<etype> : Ethernet Type: 0x600 - 0xFFFF or 'any' but excluding,
0x800(IPv4) 0x806(ARP) and 0x86DD(IPv6)

<smac> : Source MAC address (xx-xx-xx-xx-xx-xx) or 'any'

<dmac> : Destination MAC address (xx-xx-xx-xx-xx-xx) or 'any'

arp : ARP keyword

<sip> : Source IP address (a.b.c.d/n) or 'any'

<dip> : Destination IP address (a.b.c.d/n) or 'any'

<arp_opcode> : ARP operation code: any|arp|rarp|other

<arp_flags> : ARP flags: request|smac|tmac|len|ip|ether [0|1|any]

ip : IP keyword

<protocol> : IP protocol number (0-255) or 'any'

<ip_flags> : IP flags: ttl|options|fragment [0|1|any]

icmp : ICMP keyword

<icmp_type> : ICMP type number (0-255) or 'any'

<icmp_code> : ICMP code number (0-255) or 'any'

udp : UDP keyword

<sport> : Source UDP/TCP port range (0-65535) or 'any'

<dport> : Destination UDP/TCP port range (0-65535) or 'any'

tcp : TCP keyword

<tcp_flags> : TCP flags: fin|syn|rst|psh|ack|urg [0|1|any]

permit : Permit forwarding (default)

deny : Deny forwarding

<rate_limiter>: Rate limiter number (1-15) or 'disable'

<port_copy> : Port list for copy of frames or 'disable'

<mirror> : Mirror of frames: enable|disable

<logging> : System logging of frames: log|log_disable

<shutdown> : Shut down ingress port: shut|shut_disable

Security Network ACL Delete

Description:

Delete ACE.

Syntax:

Security Network ACL Delete <ace_id>

Parameters:

<ace_id>: ACE ID (1-256)

Example:

Delete ACE 1

```
NS3552-8P-2S:/>security network acl delete 1
```

Security Network ACL Lookup

Description:

Show ACE, default: All ACEs.

Syntax:

Security Network ACL Lookup [<ace_id>]

Parameters:

<ace_id>: ACE ID (1-256)

Example:

Lookup ACE 1

```
NS3552-8P-2S:/>security network acl lookup 1
```

Security Network ACL Clear

Description:

Clear all ACL counters.

Syntax:

Security Network ACL Clear

Example:

Clear all ACL counters.

```
NS3552-8P-2S:/>security network acl clear
```

Security Network ACL Status

Description:

Show ACL status.

Syntax:

Security Network ACL Status [combined|static|dhcp|upnp|arp_inspection|ipmc|ip_source_guard|conflicts]

Parameters:

combined : Shows the combined status

static : Shows the static user configured status

dhcp : Shows the status by DHCP

upnp : Shows the status by UPnP

arp_inspection : Shows the status by ARP Inspection

ip_source_guard : Shows the status by IP Source Guard

conflicts : Shows all conflict status

(default : Shows the combined status)

Example:

Show ACL status.

```
NS3552-8P-2S:/>security network acl status
```

Security Network DHCP Relay Configuration

Description:

Show DHCP relay configuration.

Syntax:

Security Network DHCP Relay Configuration

Example:

Show DHCP relay configuration.

```
NS3552-8P-2S:/>security network dhcp relay configuration

DHCP Relay Configuration:
=========================

DHCP Relay Mode             : Disabled
DHCP Relay Server           : NULL
DHCP Relay Information Mode   : Disabled
DHCP Relay Information Policy : replace
```

Security Network DHCP Relay Mode

Description:

Set or show the DHCP relay mode.

Syntax:

Security Network DHCP Relay Mode [enable|disable]

Parameters:

enable : Enable DHCP relaly mode.

When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered.

disable: Disable DHCP relaly mode

(default: Show flow DHCP relaly mode)

Default Setting:

disable

Example:

Enable DHCP relay mode

```
NS3552-8P-2S:/>security network dhcp relay mode enable
```

Security Network DHCP Relay Server

Description:

Show or set DHCP relay server.

Syntax:

Security Network DHCP Relay Server [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Show IP address

Default Setting:

null

Example:

Set DHCP relay server in 192.168.0.20

```
NS3552-8P-2S:/>security network dhcp relay server 192.168.0.20
```

Security Network DHCP Relay Information Mode

Description:

Set or show DHCP relay agent information option mode.

When enable DHCP relay information mode operation, the agent insert specific information (option 82) into a DHCP message when forwarding to DHCP server and remote it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled.

Syntax:

Security Network DHCP Relay Information Mode [enable|disable]

Parameters:

enable : Enable DHCP relay agent information option mode

disable: Disable DHCP relay agent information option mode

(default: Show DHCP relay agent information option mode)

Default Setting:

disable

Example:

Enable DHCP relay agent information option mode.

```
NS3552-8P-2S:/>security network dhcp relay information mode enable
```

Security Network DHCP Relay Information Policy

Description:

Set or show the DHCP relay mode.

When enable DHCP relay information mode operation, if agent receive a DHCP message that already contains relay agent information. It will enforce the policy.

Syntax:

Security Network DHCP Relay Information Policy [replace|keep|drop]

Parameters:

replace : Replace the original relay information when receive a DHCP message that already contains it

keep : Keep the original relay information when receive a DHCP message that already contains it

drop : Drop the package when receive a DHCP message that already contains relay information

(default: Show DHCP relay information policy)

Default Setting:

replace

Example:

Keep the original relay information when receive a DHCP message that already contains it

```
NS3552-8P-2S:/>security network dhcp relay information policy keep
```

Security Network DHCP Relay Statistics

Description:

Show or clear DHCP relay statistics.

Syntax:

Security Network DHCP Relay Statistics [clear]

Parameters:

clear: Clear DHCP relay statistics

Example:

Show DHCP relay statistics.

```
NS3552-8P-2S:/>security network dhcp relay statistics
```

Security Network DHCP Snooping Configuration

Description:

Show DHCP snooping configuration.

Syntax:

Security Network DHCP Snooping Configuration

Security Network DHCP Snooping Mode

Description:

Set or show the DHCP snooping mode.

Syntax:

Security Network DHCP Snooping Mode [enable|disable]

Parameters:

enable : Enable DHCP snooping mode.

When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports.

disable: Disable DHCP snooping mode

(default: Show flow DHCP snooping mode)

Default Setting:

disable

Example:

Enable DHCP snooping mode

```
NS3552-8P-2S:/>security network dhcp snooping mode enable
```

Security Network DHCP Snooping Port Mode

Description:

Set or show the DHCP snooping port mode.

Syntax:

Security Network DHCP Snooping Port Mode [<port_list>] [trusted|untrusted]

Parameters:

<port_list>: Port list or 'all', default: All ports

trusted : Configures the port as trusted sources of the DHCP message

untrusted: Configures the port as untrusted sources of the DHCP message

(default: Show flow DHCP snooping port mode)

Default Setting:

trusted

Example:

Set untrusted DHCP snooping port mode in port 1

```
NS3552-8P-2S:/>security network dhcp snooping port mode 1 untrusted
```

Security Network DHCP Snooping Statistics

Description:

Show or clear DHCP snooping statistics.

Syntax:

Security Network DHCP Snooping Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear DHCP snooping statistics

Example:

Show DHCP snooping statistics of port 1.

```
NS3552-8P-2S:/>security network dhcp snooping statistics 1
Port 1 Statistics:
--------------------
Rx Discover:              0   Tx Discover:              0
Rx Offer:                 0   Tx Offer:                 0
Rx Request:               0   Tx Request:               0
Rx Decline:               0   Tx Decline:               0
Rx ACK:                   0   Tx ACK:                   0
Rx NAK:                   0   Tx NAK:                   0
Rx Release:               0   Tx Release:               0
Rx Inform:                0   Tx Inform:                0
Rx Lease Query:           0   Tx Lease Query:           0
Rx Lease Unassigned:      0   Tx Lease Unassigned:      0
Rx Lease Unknown:         0   Tx Lease Unknown:         0
Rx Lease Active:          0   Tx Lease Active:          0
```

Security Network IP Source Guard Configuration

Description:

Show IP source guard configuration.

Syntax:

Security Network IP Source Guard Configuration

Security Network IP Source Guard Mode

Description:

Set or show IP source guard mode.

Syntax:

Security Network IP Source Guard Mode [enable|disable]

Parameters:

enable : Enable IP Source Guard

disable: Disable IP Source Guard

Default Setting:

disable

Example:

Enable IP source guard mode

```
NS3552-8P-2S:/>security network ip source guard mode enable
```

Security Network IP Source Guard Port Mode

Description:

Set or show the IP Source Guard port mode.

Syntax:

Security Network IP Source Guard Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable IP Source Guard port

disable : Disable IP Source Guard port

(default: Show IP Source Guard port mode)

Default Setting:

disable

Example:

Enable IP source guard port mode for port1~4

```
NS3552-8P-2S:/>security network ip source guard port mode 1-4 enable
```

Security Network IP Source Guard Limit

Description:

Set or show the IP Source Guard port limitation for dynamic entries.

Syntax:

Security Network IP Source Guard limit [<port_list>] [<dynamic_entry_limit>|unlimited]

Parameters:

<port_list> : Port list or 'all', default: All ports

<dynamic_entry_limit>|unlimited: dynamic entry limit (0-2) or unlimited

Default Setting:

unlimited

Example:

Set IP source guard limit

```
NS3552-8P-2S:/>security network ip source guard 1 1
```

Security Network IP Source Guard Entry

Description:

Add or delete IP source guard static entry.

Syntax:

Security Network IP Source Guard Entry [<port_list>] add|delete <vid> <allowed_ip> <allowed_mac>

Parameters:

<port_list> : Port list or 'all', default: All ports

add : Add new port IP source guard static entry

delete : Delete existing port IP source guard static entry

<vid> : VLAN ID (1-4095)

<allowed_ip> : IP address (a.b.c.d), IP address allowed for doing IP source guard

<allowed_mac>: MAC address (xx-xx-xx-xx-xx-xx), MAC address allowed for doing IP source guard

Example:

Add IP source guard static entry.

```
NS3552-8P-2S:/>security network ip source guard entry 1 add 1 192.168.0.20
```

Security Network IP Source Guard Status

Description:

Show IP source guard static and dynamic entries.

Syntax:

Security Network IP Source Guard Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show IP source guard static and dynamic entries.

```
NS3552-8P-2S:/>security network ip source guard status
```

Security Network IP Source Guard Translation

Description:

Translate IP source guard dynamic entries into static entries.

Syntax:

Security Network IP Source Guard Translation

Security Network ARP Inspection Configuration

Description:

Show ARP inspection configuration.

Syntax:

Security Network ARP Inspection Configuration

Example:

Show ARP inspection configuration.

```
NS3552-8P-2S:/>security network arp inspection configuration
```

Security Network ARP Inspection Mode

Description:

Set or show ARP inspection mode.

Syntax:

Security Network ARP Inspection Mode [enable|disable]

Parameters:

enable : Enable ARP Inspection

disable: Disable ARP Inspection

Default Setting:

disable

Example:

Enable ARP inspection mode

```
NS3552-8P-2S:/>security network arp inspection mode enable
```

Security Network ARP Inspection Port Mode

Description:

Set or show the ARP Inspection port mode.

Syntax:

Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable ARP Inspection port

disable : Disable ARP Inspection port

(default: Show ARP Inspection port mode)

Default Setting:

Disable

Example:

Enable the ARP inspection mode of port 1

```
NS3552-8P-2S:/>security network arp inspection port mode 1
```

Security Network ARP Inspection Entry

Description:

Add or delete ARP inspection static entry.

Syntax:

Security Network ARP Inspection Entry [<port_list>] add|delete <vid> <allowed_mac> <allowed_ip>

Parameters:

<port_list> : Port list or 'all', default: All ports

add : Add new port ARP inspection static entry

delete : Delete existing port ARP inspection static entry

<vid> : VLAN ID (1-4095)

<allowed_mac>: MAC address (xx-xx-xx-xx-xx-xx), MAC address allowed for doing ARP request

<allowed_ip> : IP address (a.b.c.d), IP address allowed for doing ARP request

Example:

Add ARP inspection static entry.

```
NS3552-8P-2S:/>security network arp inspection entry 1 add 1 00-30-4f-00-00-11 192.168.0.11
```

Security Network ARP Inspection Status

Description:

Show ARP inspection static and dynamic entries.

Syntax:

Security Network ARP Inspection Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show ARP inspection static and dynamic entries.

```
NS3552-8P-2S:/>security network arp inspection status
```

Security Network ARP Inspection Translation

Description:

Translate ARP inspection dynamic entries into static entries.

Syntax:

Security Network ARP Inspection Translation

Security AAA Configuration

Description:

Show Auth configuration.

Syntax:

Security AAA Configuration

Example:

Show Auth configuration.

```
NS3552-8P-2S:/>security aaa configuration

AAA Configuration:
==================


Server Timeout   : 15 seconds

Server Dead Time : 300 seconds
```

```
RADIUS Authentication Server Configuration:
=========================================
Server  Mode     IP Address      Secret                    Port
------  --------  ---------------  ------------------------------  -----
1       Disabled                                  1812
2       Disabled                                  1812
3       Disabled                                  1812
4       Disabled                                  1812
5       Disabled                                  1812

RADIUS Accounting Server Configuration:
=======================================
Server  Mode     IP Address      Secret                    Port
------  --------  ---------------  ------------------------------  -----
1       Disabled                                  1813
2       Disabled                                  1813
3       Disabled                                  1813
4       Disabled                                  1813
5       Disabled                                  1813

TACACS+ Authentication Server Configuration:
============================================
Server  Mode     IP Address      Secret                    Port
------  --------  ---------------  ------------------------------  -----
1       Disabled                                    49
2       Disabled                                    49
3       Disabled                                    49
4       Disabled                                    49
5       Disabled                                    49
```

Security AAA Timeout

Description:

Set or show server timeout.

Syntax:

Security AAA Timeout [<timeout>]

Parameters:

<timeout>: Server response timeout (3-3600 seconds)

(default: Show server timeout configuration)

Default Setting:

15

Example:

Set 30sec for server timeout

```
NS3552-8P-2S:/>security aaa timeout 30
```

Security AAA Deadtime

Description:

Set or show server dead time.

Syntax:

Security AAA Deadtime [<dead_time>]

Parameters:

<dead_time>: Time that a server is considered dead if it doesn't answer a request (0-3600 seconds)

(default: Show server dead time configuration)

Default Setting:

300

Example:

Set 1000sec for server dead time

```
NS3552-8P-2S:/>security aaa deadtime 1000
```

Security AAA RADIUS

Description:

Set or show RADIUS authentication server setup.

Syntax:

Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)

(default: Show RADIUS authentication server configuration)

enable : Enable RADIUS authentication server

disable : Disable RADIUS authentication server

(default: Show RADIUS server mode)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<secret> : Secret shared with external authentication server.

To set an empty secret, use two quotes ("").

To use spaces in secret, enquote the secret.

Quotes in the secret are not allowed.

<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1812)

Example:

Set RADIUS authentication server configuration.

```
NS3552-8P-2S:/>security aaa radius 1 enable 192.168.0.20 12345678 1812
```

Security AAA ACCT_RADIUS

Description:

Set or show RADIUS accounting server setup.

Syntax:

Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)

(default: Show RADIUS accounting server configuration)

enable : Enable RADIUS accounting server

disable : Disable RADIUS accounting server

(default: Show RADIUS server mode)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<secret> : Secret shared with external accounting server.

To set an empty secret, use two quotes ("").

To use spaces in secret, enquote the secret.

Quotes in the secret are not allowed.

<server_port> : Server UDP port. Use 0 to use the default RADIUS port (1813)

Example:

Set RADIUS accounting server configuration.

```
NS3552-8P-2S:/>security acct_radius 1 enable 192.168.0.20 12345678 1813
```

Security AAA TACACS+

Description:

Set or show TACACS+ authentication server setup.

Syntax:

Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)

(default: Show TACACS+ authentication server configuration)

enable : Enable TACACS+ authentication server

disable : Disable TACACS+ authentication server

(default: Show TACACS+ server mode)

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<secret> : Secret shared with external authentication server.

To set an empty secret, use two quotes ("").

To use spaces in secret, enquote the secret.

Quotes in the secret are not allowed.

<server_port> : Server TCP port. Use 0 to use the default TACACS+ port (49)

Example:

Set TACACS+ authentication server configuration.

```
NS3552-8P-2S:/>security aaa tacacs+ 1 enable 192.168.0.20 12345678 49
```

Security AAA Statistics

Description:

Show RADIUS statistics.

Syntax:

Security AAA Statistics [<server_index>]

Parameters:

The server index (1-5)

(default: Show statistics for all servers)

Example:

Show RADIUS statistics.

```
NS3552-8P-2S:/>security aaa statistics
```

6.8 Spanning Tree Protocol Command

STP Configuration

Description:

Show STP configuration.

Syntax:

STP Configuration

Example:

Show STP configuration.

```
NS3552-8P-2S:/>stp cofiguration

STP Configuration:
==================

Protocol Version: MSTP
Max Age         : 20
Forward Delay   : 15
Tx Hold Count   : 6
Max Hop Count   : 20
BPDU Filtering  : Disabled
BPDU Guard      : Disabled
Error Recovery  : Disabled
```

STP Version

Description:

Set or show the STP Bridge protocol version.

Syntax:

STP Version [<stp_version>]

Parameters:

<stp_version>: mstp|rstp|stp

Default Setting:

MSTP

Example:

Set the STP Bridge protocol version.

```
NS3552-8P-2S:/> stp version rstp
```

STP Tx Hold

Description:

Set or show the STP Bridge Transmit Hold Count parameter.

Syntax:

STP Txhold [<holdcount>]

Parameters:

<holdcount>: STP Transmit Hold Count (1-10)

Default Setting:

6

Example:

Set STP Tx hold in 10

```
NS3552-8P-2S:/>stp txhold 10
```

STP MaxHops

Description:

Set or show the MSTP Bridge Max Hop Count parameter.

Syntax:

STP MaxHops [<maxhops>]

Parameters:

<maxhops>: STP BPDU MaxHops (6-40))

Default Setting:

20

Example:

Set STP maximum hops in 25

```
NS3552-8P-2S:/>stp maxhops 25
```

STP MaxAge

Description:

Set or show the bridge instance maximum age.

Syntax:

STP MaxAge [<max_age>]

Parameters:

<max_age>: STP maximum age time (6-40, and max_age <= (forward_delay-1)*2)

Default Setting:

20

Example:

Set STP maximum age time in 10

```
NS3552-8P-2S:/>stp maxage 10
```

STP FwdDelay

Description:

Set or show the CIST/MSTI bridge forward delay.

Syntax:

STP FwdDelay [<delay>]

Parameters:

<delay>: MSTP forward delay (4-30, and max_age <= (forward_delay-1)*2))

Default Setting:

15

Example:

Set STP forward delay value in 25

```
NS3552-8P-2S:/>stp fwddelay 25
```

STP CName

Description:

Set or Show MSTP configuration name and revision.

Syntax:

STP CName [<config-name>] [<integer>]

Parameters:

<config-name>: MSTP Configuration name. A text string up to 32 characters long.

Use quotes (") to embed spaces in name.

<integer> : Integer value

Default Setting:

Configuration name: MAC address

Configuration rev.: 0

Example:

Set MSTP configuration name and revision.

```
NS3552-8P-2S:/>stp cname 9f_NS3552-8P-2S 1
```

STP BPDU Filter

Description:

Set or show edge port BPDU Filtering.

Syntax:

STP bpduFilter [enable|disable]

Parameters:

enable|disable: enable or disable BPDU Filtering for Edge ports

Default Setting:

Disable

Example:

Set edge port BPDU filtering

```
NS3552-8P-2S:/>stp bpdufilter enable
```

STP BPDU Guard

Description:

Set or show edge port BPDU Guard.

Syntax:

STP bpduGuard [enable|disable]

Parameters:

enable|disable: enable or disable BPDU Guard for Edge ports

Default Setting:

Disable

Example:

Set edge port BPDU guard

```
NS3552-8P-2S:/>stp bpduguard enable
```

STP Recovery

Description:

Set or show edge port error recovery timeout.

Syntax:

STP recovery [<timeout>]

Parameters:

<timeout>: Time before error-disabled ports are reenabled (30-86400 seconds, 0 disables)

(default: Show recovery timeout)

Default Setting:

Disable

Example:

Set STP recovery value in 30 sec.

```
NS3552-8P-2S:/>stp recovery 30
```

STP Status

Description:

Show STP Bridge status.

Syntax:

STP Status [<msti>] [<port_list>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list>: Port list or 'all', default: All ports

Default Setting:

Disable

Example:

Show STP Bridge status.

```
NS3552-8P-2S:/>stp status
CIST Bridge STP Status
```

```
Bridge ID    : 80:00-00:30:4F:24:04:D1
Root ID      : 80:00-00:30:4F:24:04:D1
Root Port    : -
Root PathCost: 0
Regional Root: 80:00-00:30:4F:24:04:D1
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 0
TC Last      : -
Port      Port Role      State      Pri  PathCost  Edge  P2P  Uptime
---------  --------------  ----------  ---  --------  ----  ---  -------------
10      DesignatedPort  Forwarding  128  20000     Yes   Yes  0d 00:10:32
```

STP MSTI Priority

Description:

Set or show the bridge instance priority.

Syntax:

STP Msti Priority [<msti>] [<priority>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<priority> : STP bridge priority (0/16/32/48/.../224/240)

Default:

128

Example:

Set MST1 priority value in 48.

```
NS3552-8P-2S:/>stp msti priority 1 48
```

STP MSTI Map

Description:

Show or clear MSTP MSTI VLAN mapping configuration.

Syntax:

STP Msti Map [<msti>] [clear]

Parameters:

<msti>: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

Clear : Clear VID to MSTI mapping

Example:

Add MST1 priority value in 48.

```
NS3552-8P-2S:/>stp msti priority 1 48
```

STP MSTI Add

Description:

Add a VLAN to a MSTI.

Syntax:

STP Msti Add <msti> <vid>

Parameters:

<msti>: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<vid> : VLAN ID (1-4095)

Example:

Add MST1 in vlan1.

```
NS3552-8P-2S:/>stp msti add 1 1
```

STP Port Configuration

Description:

Show STP Port configuration.

Syntax:

STP Port Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

Example:

Show STP status of Port1

```
NS3552-8P-2S:/>stp port configuration 1

Port  Mode     AdminEdge AutoEdge  restrRole restrTcn  Point2point
----  -------- ----------------- ----------------- -----------
1     Disabled  Disabled  Enabled   Disabled  Disabled  Auto
```

STP Port Mode

Description:

Set or show the STP enabling for a port.

Syntax:

STP Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all'. Port zero means aggregations.

Enable : Enable MSTP protocol

Disable : Disable MSTP protocol

Default:

disable

Example:

Enable STP function on port1

```
NS3552-8P-2S:/>stp port mode 1 enable
```

STP Port Edge

Description:

Set or show the STP adminEdge port parameter.

Syntax:

STP Port Edge [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

Enable : Configure MSTP adminEdge to Edge

Disable : Configure MSTP adminEdge to Non-edge

Default:

disable

Example:

Enable STP edge function on port1

```
NS3552-8P-2S:/>stp port edge 1 enable
```

STP Port AutoEdge

Description:

Set or show the STP autoEdge port parameter.

Syntax:

STP Port AutoEdge [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

Enable : Enable MSTP autoEdge

Disable : Disable MSTP autoEdge

Default:

enable

Example:

Disable STP edge function on port1

```
NS3552-8P-2S:/>stp port autoedge 1 disable
```

STP Port P2P

Description:

Set or show the STP point2point port parameter.

Syntax:

STP Port P2P [<port_list>] [enable|disable|auto]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable MSTP point2point

disable : Disable MSTP point2point

auto : Automatic MSTP point2point detection

Default:

auto

Example:

Disable STP P2P function on port1

```
NS3552-8P-2S:/>stp port p2p 1 disable
```

STP Port RestrictedRole

Description:

Set or show the MSTP restrictedRole port parameter.

Syntax:

STP Port RestrictedRole [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable MSTP restricted role

disable : Disable MSTP restricted role

Default:

disable

Example:

Eisable STP restricted role on port1

```
NS3552-8P-2S:/>stp port restrictedrole 1 enable
```

STP Port RestrictedTcn

Description:

Set or show the MSTP restrictedTcn port parameter.

Syntax:

STP Port RestrictedTcn [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable MSTP restricted TCN

disable : Disable MSTP restricted TCN

Default:

disable

Example:

Eisable STP restricted TCN on port1

```
NS3552-8P-2S:/>stp port restrictedtcn 1 enable
```

STP Port bpduGuard

Description:

Set or show the bpduGuard port parameter.

Syntax:

STP Port bpduGuard [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port BPDU Guard

disable : Disable port BPDU Guard

Default:

disable

Example:

Eisable BPDU guard on port1

```
NS3552-8P-2S:/>stp port bpduguard 1 enable
```

STP Port Statistic

Description:

Show STP port statistics.

Syntax:

STP Port Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear the selected port statistics

Example:

Show STP port statistics.

```
NS3552-8P-2S:/>stp port statistics
Port     Rx MSTP   Tx MSTP   Rx RSTP   Tx RSTP   Rx STP   Tx STP   Rx TCN   Tx TCN   Rx Ill.
Rx Unk.
---------  --------  --------  --------  --------  -------  -------  -------  -------  -------  -------
```

STP Port Mcheck

Description:

Set the STP mCheck (Migration Check) variable for ports.

Syntax:

STP Port Mcheck [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Set the STP mCheck (Migration Check) variable for port 1.

```
NS3552-8P-2S:/>stp port mcheck 1
```

STP MSTI Port Configuration

Description:

Show the STP port instance configuration.

Syntax:

STP Msti Port Configuration [<msti>] [<port_list>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list>: Port list or 'all', default: All ports

Default:

auto

STP MSTI Port Cost

Description:

Set or show the STP port instance path cost.

Syntax:

STP Msti Port Cost [<msti>] [<port_list>] [<path_cost>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list>: Port list or 'all'. Port zero means aggregations.

<path_cost>: STP port path cost (1-200000000) or 'auto'

Default:

auto

Example:

Set MSTI7 in port1

```
NS3552-8P-2S:/>stp msti port cost 7 1

MSTI  Port  Path Cost
----  ----  ----------
MST7  1     Auto
```

STP MSTI Port Priority

Description:

Set or show the STP port instance priority.

Syntax:

STP Msti Port Priority [<msti>] [<port_list>] [<priority>]

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

<port_list>: Port list or 'all'. Port zero means aggregations.

<priority> : STP port priority (0/16/32/48/.../224/240)

Default:

128

6.9 Link Aggregation Command

Aggregation Configuration

Description:

Show link aggregation configuration.

Syntax:

Aggr Configuration

Aggregation Add

Description:

Add or modify link aggregation.

Syntax:

Aggr Add <port_list> [<aggr_id>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<aggr_id> : Aggregation ID

Example:

Add port 1~4 in Group1

```
NS3552-8P-2S:/>aggr add 1-4 1
```

Aggregation Delete

Description:

Delete link aggregation.

Syntax:

Aggr Delete <aggr_id>

Parameters:

<aggr_id>: Aggregation ID

Example:

Delete Group2

```
NS3552-8P-2S:/>aggr delete 2
```

Aggregation Lookup

Description:

Lookup link aggregation.

Syntax:

Aggr Lookup [<aggr_id>]

Parameters:

<aggr_id>: Aggregation ID

Aggregation Mode

Description:

Set or show the link aggregation traffic distribution mode.

Syntax:

Aggr Mode [smac|dmac|ip|port] [enable|disable]

Parameters:

smac : Source MAC address

dmac : Destination MAC address

ip : Source and destination IP address

port : Source and destination UDP/TCP port

enable : Enable field in traffic distribution

disable: Disable field in traffic distribution

Default Setting:

SMAC : Enabled

DMAC : Disabled

IP : Enabled

Port : Enabled

Example:

Disable SMAC mode

```
NS3552-8P-2S:/>Aggr mode smac disable
```

6.10 Link Aggregation Control Protocol Command

LACP Configuration

Description:

Show LACP configuration.

Syntax:

LACP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP configuration

```
NS3552-8P-2S:/>lacp configuration

Port  Mode     Key   Role
----  --------    ----   ------
1     Disabled  Auto  Active
2     Disabled  Auto  Active
3     Disabled  Auto  Active
4     Disabled  Auto  Active
5     Disabled  Auto  Active
6     Disabled  Auto  Active
7     Disabled  Auto  Active
8     Disabled  Auto  Active
9     Disabled  Auto  Active
10    Disabled  Auto  Active
```

LACP Mode

Description:

Set or show LACP mode.

Syntax:

LACP Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable LACP protocol

disable: Disable LACP protocol

(default: Show LACP mode)

Default Setting:

disable

Example:

Enable LACP for port1~4

```
NS3552-8P-2S:/>lacp mode 1-4 enable
```

LACP Key

Description:

Set or show the LACP key.

Syntax:

LACP Key [<port_list>] [<key>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<key> : LACP key (1-65535) or 'auto'

Default Setting:

auto

Example:

Set key1 for port1~4

```
NS3552-8P-2S:/>lacp key 1-4 1
```

LACP Prio

Description:

Set or show the LACP prio.

Syntax:

LACP Prio [<port_list>] [<prio>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<prio> : LACP Prio (0-65535)

Default Setting:

32768

LACP System Prio

Description:

Set or show the LACP System prio.

Syntax:

LACP System Prio [<sysprio>]

Parameters:

<sysprio>: LACP System Prio (0-65535)

Default Setting:

32768

LACP Role

Description:

Set or show the LACP role.

Syntax:

LACP Role [<port_list>] [active|passive]

Parameters:

<port_list>: Port list or 'all', default: All ports

active : Initiate LACP negotiation

passive: Listen for LACP packets

(default: Show LACP role)

Default Setting:

active

Example:

Set passive for port1~4

```
NS3552-8P-2S:/>lacp role 1-4 passive
```

LACP Status

Description:

Show LACP Status.

Syntax:

LACP Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LACP status of port1~4

```
NS3552-8P-2S:/>lacp status 1-4

Port  Mode      Key   Aggr ID  Partner System ID  Partner Port
----  --------  ----- -------  -----------------  ------------
1     Disabled  1     -        -                  -
2     Disabled  1     -        -                  -
3     Disabled  1     -        -                  -
4     Disabled  1     -        -                  -
```

LACP Statistics

Description:

Show LACP Statistics.

Syntax:

LACP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear **:** Clear LACP statistics

Example:

Show LACP statistics of port1~4

```
NS3552-8P-2S:/>lacp statistics 1-4

Port  Rx Frames   Tx Frames   Rx Unknown  Rx Illegal
------ ---------- ---------- ---------- ----------
1     0          0          0          0
2     0          0          0          0
3     0          0          0          0
4     0          0          0          0
```

LACP Timeout

Description:

Set or show the LACP timeout.

Syntax:

LACP Timeout [<port_list>] [fast|slow]

Parameters:

<port_list>: Port list or 'all', default: All ports

fast : Fast PDU transmissions (fast timeout)

slow : Slow PDU transmissions (slow timeout)

(default: Show LACP timeout)

Default Setting:

fast

6.11 LLDP Command

LLDP Configuration

Description:

Show LLDP configuration.

Syntax:

LLDP Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LLDP configuration of port1~4

```
NS3552-8P-2S:/>lldp configuration 1-4

LLDP Configuration:
===================

Interval    : 30
Hold        : 3
Tx Delay    : 2
Reinit Delay: 2

Port Mode     Port Descr System Name System Descr System Capa Mgmt Addr CDP awareness
---- -------- ---------- ----------- ------------ ----------- --------- -------------
1    Enabled  Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
2    Enabled  Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
3    Enabled  Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
4    Enabled  Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
```

LLDP Mode

Description:

Set or show LLDP mode.

Syntax:

LLDP Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable LLDP reception and transmission

disable: Disable LLDP

rx : Enable LLDP reception only

tx : Enable LLDP transmission only

(default: Show LLDP mode)

Default Setting:

disable

Example:

Enable port1 LLDP function.

```
NS3552-8P-2S:/>lldp mode 1 enable
```

LLDP Optional TLV

Description:

Show or Set LLDP Optional TLVs.

Syntax:

LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

port_descr : Description of the port

sysm_name : System name

sys_descr : Description of the system

sys_capa : System capabilities

mgmt_addr : Master's IP address

(default: Show optional TLV's configuration)

enable : Enables TLV

disable : Disable TLV

(default: Show optional TLV's configuration)

Default Setting:

Description of the port: Enable

System name: Enable

Description of the system: Enable

System capabilities: Enable

Master's IP address: Enable

Example:

Disable description of the port for port1

```
NS3552-8P-2S:/>lldp optional_tlv 1 port_descr disable
```

LLDP Interval

Description:

Set or show LLDP Tx interval.

Syntax:

LLDP Interval [<interval>]

Parameters:

<interval>: LLDP transmission interval (5-32768)

Default Setting:

30

Example:

Set transmission interval in 10

```
NS3552-8P-2S:/>lldp interval 10
```

LLDP Hold

Description:

Set or show LLDP Tx hold value.

Syntax:

LLDP Hold [<hold>]

Parameters:

<hold>: LLDP hold value (2-10)

Default Setting:

3

Example:

Set LLDP hold value in 10

```
NS3552-8P-2S:/>lldp hold 10
```

LLDP Delay

Description:

Set or show LLDP Tx delay.

Syntax:

LLDP Delay [<delay>]

Parameters:

<delay>: LLDP transmission delay (1-8192)

Default Setting:

2

Example:

Set LLDP delay value in 1

```
NS3552-8P-2S:/>lldp delay 1
```

LLDP Reinit

Description:

Set or show LLDP reinit delay.

Syntax:

LLDP Reinit [<reinit>]

Parameters:

<reinit>: LLDP reinit delay (1-10)

Default Setting:

2

Example:

Set LLDP reinit delay value in 3

```
NS3552-8P-2S:/>lldp reinit 3
```

LLDP Statistics

Description:

Show LLDP Statistics.

Syntax:

LLDP Statistics [<port_list>] [clear]

Parameters:

<port_list>: Port list or 'all', default: All ports

clear : Clear LLDP statistics

Example:

Show LLDP Statistics of port 1

```
NS3552-8P-2S:/>lldp statistics 1

LLDP global counters
Neighbor entries was last changed at - (18819 sec. ago).
Total Neighbors Entries Added    0.
Total Neighbors Entries Deleted  0.
Total Neighbors Entries Dropped  0.
Total Neighbors Entries Aged Out 0.

LLDP local counters
      Rx       Tx       Rx       Rx       Rx TLV   Rx TLV   Rx TLV
Port  Frames   Frames   Errors   Discards Errors   Unknown  Organz.  Aged
----  ------   ------   ------   --------  ------   -------  -------  -----
1     0        0        0        0         0        0        0        0
```

LLDP Info

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

6.12 LLDP MED Command

LLDP MED Configuration

Description:

Show LLDP-MED configuration.

Syntax:

LLDPMED Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show LLDP-MED configuration of port1~4

```
NS3552-8P-2S:/>lldpmed configuration 1-4

LLDP-MED Configuration:
=======================

Fast Start Repeast Count : 4
Location Coordinates    : Latitude              - 0.0000 North
                          Longitude             - 0.0000 East
                          Altitude              - 0.0000 meter(s)
                          Map datum             - WGS84
Civic Address Location  :


Port      Policies
1         none
2         none
3         none
4         none
```

LLDP MED Civic

Description:

Set or show LLDP-MED Civic Address Location.

Syntax:

LLDPMED Civic [country|state|county|city|district|block|street|leading_street_direction|trailing_street_suffix|str_suf|house_no|house_no_suffix|landmark|additional_info|name|zip_code|building|apartment|floor|room_number|place_type|postal_com_name|p_o_box|additional_code] [<civic_value>]

Parameters:

country : Country

state : National subdivisions (state, caton, region, province, prefecture)

county : County, parish,gun (JP), district(IN)

city : City, townchip, shi (JP)

district : City division,borough, city, district, ward,chou (JP)

block : Neighborhood, block

street : Street

leading_street_direction : Leading street direction

trailing_street_suffix : Trailing street suffix

str_suf : Street Suffix

house_no : House Number

house_no_suffix : House number suffix

landmark : Landmark or vanity address

additional_info : Additional location information

name : Bame(residence and office occupant)

zip_code : Postal/zip code

building : Building (structure)

apartment : Unit (apartment, suite)

floor : Floor

room_number : Room numbe**r**

place_type : Placetype

postal_com_name : Postal community name

p_o_box : Post office box (P.O. Box)

additional_code : Addtional code

(default: Show Civic Address Location configuration)

<civic_value>: lldpmed The value for the Civic Address Location entry.

LLDP MED ECS

Description:

Set or show LLDP-MED Emergency Call Service.

Syntax:

LLDPMED ecs [<ecs_value>]

Parameters:

<ecs_value>: lldpmed The value for the Emergency Call Service

LLDP MED Policy Delete

Description:

Delete the selected policy.

Syntax:

LLDPMED policy delete [<policy_list>]

Parameters:

<policy_list>: List of policies to delete

Example:

Delete the policy 1

```
NS3552-8P-2S:/>lldpmed policy delete 1
```

LLDP MED Policy Add

Description:

Adds a policy to the list of polices.

Syntax:

LLDPMED policy add [voice|voice_signaling|guest_voice|guest_voice_signaling|softphone_voice|video_conferencing|streaming_video|video_signaling] [tagged|untagged] [<vlan_id>] [<l2_priority>] [<dscp>]

Parameters:

voice : Voice for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications

voice_signaling : Voice Signaling (conditional) for use in network topologies that require a different policy for the voice signaling than for the voice media.

guest_voice : Guest Voice to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

guest_voice_signaling : Guest Voice Signaling (conditional) for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.

softphone_voice : Softphone Voice for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all,and are typically configured to use an untagged VLAN or a single tagged data specific VLAN.

video_conferencing : Video Conferencing for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

streaming_video : Streaming Video for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

video_signaling : Video Signaling (conditional) for use in network topologies that require a separate policy for the video signaling than for the video media.

tagged : The device is using tagged frames

unragged : The device is using untagged frames

<vlan_id> : VLAN id

<l2_priority>: This field may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004 [3].

<dscp> : This field shall contain the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474 [5]. This 6 bit field may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

LLDP MED Port Policy

Description:

Set or show LLDP-MED port polcies.

Syntax:

LLDPMED port policies [<port_list>] [<policy_list>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<policy_list>: List of policies to delete

LLDP MED Coordinates

Description:

Set or show LLDP-MED Location.

Syntax:

LLDPMED Coordinates [latitude|longitude|altitude] [north|south|west|east|meters|floor] [coordinate_value]

Parameters:

latitude : Latitude, 0 to 90 degress with max. 4 digits (Positive numbers are north of the equator and negative numbers are south of the equator).

longitude : Longitude,0 to 180 degress with max. 4 digits (Positive values are East of the prime meridian and negative numbers are West of the prime meridian.

altitude : Altitude, Meters or floors with max. 4 digits.

(default: Show coordinate location configuration)

north|south|west|east|meters|floor:

North : North (Valid for latitude)

South : South (Valid for latitude)

West : West (Valid for longitude)

East : East (Valid for longitude)

Meters : Meters (Valid for altitude)

Floor : Floor (Valid for altitude)

lldpmed Coordinate value

coordinate_value : lldpmed Coordinate value

LLDP MED Datum

Description:

Set or show LLDP-MED Coordinates map datum.

Syntax:

LLDPMED Datum [wgs84|nad83_navd88|nad83_mllw]

Parameters:

wgs84|nad83_navd88|nad83_mllw:

wgs84 : WGS84

nad83_navd88 : NAD83_NAVD88

nad83_mllw : NAD83_MLLW

lldpmed Coordinate datum

LLDP MED Fast

Description:

Set or show LLDP-MED Fast Start Repeat Count.

Syntax:

LLDPMED Fast [<count>]

Parameters:

<count>: The number of times the fast start LLDPDU are being sent during the activation of the fast start mechanism defined by LLDP-MED (1-10).

LLDP MED Info

Description:

Show LLDP-MED neighbor device information.

Syntax:

LLDPMED Info [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

6.13 EEE Command

EEE Configuration

Description:

Show eee configuration.

Syntax:

EEE Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show EEE configuration of port1~4

```
NS3552-8P-2S:/>eee configuration 1-4

EEE Configuration:
==================


Port  Mode     Urgent queues
----  -------  -------------
1     Disabled none
2     Disabled none
3     Disabled none
4     Disabled none
```

EEE Mode

Description:

Set or show the eee mode.

Syntax:

EEE Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable EEE

disable: Disable EEE

(default: Show eee mode)

Default Setting:

Disabled

Example:

Enable EEE mode for port1~4

```
NS3552-8P-2S:/>eee mode enable 1-4
```

EEE Urgent Queues

Description:

Set or show EEE Urgent queues.

Syntax:

EEE Urgent_queues [<port_list>] [<queue_list>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<queue_list>: List of queues to configure as urgent queues (1-8 or none)

Default Setting:

None

6.14 Thermal Command

Thermal Prio_temp

Description:

Set or show the temperature at which the ports shall be shut down.

Syntax:

Thermal prio_temp [<prio_list>] [<shut_down_temp>]

Parameters:

<prio_list> : List of priorities (0-3)

<shut_down_temp>: Temperature at which ports shall be shut down (0-255 degree C)

Thermal Port_prio

Description:

Set or show the ports priority.

Syntax:

Thermal port_prio [<port_list>] [<prio>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<prio> : Priority (0-3)

Thermal Status

Description:

Shows the chip temperature.

Syntax:

Thermal status

Thermal Configuration

Description:

Show thermal_protect configuration.

Syntax:

Thermal configuration

6.15 PoE Command (NS3552-8P-2S only)

PoE Configuration

Description:

Show PoE configuration.

Syntax:

PoE Configuration

PoE Mode

Description:

Set or show the PoE mode.

Syntax:

PoE Mode [<port_list>] [enable|disable] [af|at]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enables PoE

disable : Disable PoE

(default: Show PoE's mode)

af : PoE to af mode

at : PoE to at mode

(default: Show PoE's af/at mode)

Default Setting:

enable

PoE Priority

Description:

Show / Set PoE Priority.

Syntax:

PoE Priority [<port_list>] [low|high|critical]

Parameters:

<port_list>: Port list or 'all', default: All ports

low : Set priority to low

high : Set priority to high

critical: Set priority to critical

(default: Show PoE priority)

Default Setting:

high

PoE Mamagement Mode

Description:

Show / Set PoE management mode.

Syntax:

PoE Mgmt_mode [mgt_class|mgt_alloc|mgt_consumption|mgt_priority]

PoE Allocated Power

Description:

Set or show PoE maximum power allocated per port (0-30.8, with one digit).

Syntax:

PoE Alloc_Power [<port_list>] [<alloc_power>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<alloc_power>: PoE maiximum power allocated for the port (0-30.8)

Default Setting:

30.8

PoE Power Supply

Description:

Set or show the value of the power supply.

Syntax:

PoE Power_Supply [<supply_power>]

Parameters:

<supply_power>: PoE power for a power supply

PoE Status

Description:

Show PoE status.

Syntax:

PoE Status

6.16 Ethernet Virtual Connections Command

EVC Configuration

Description:

Show EVC configuration.

Syntax:

EVC Configuration [<port_list>] [<policer_id>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<policer_id>: Policer ID (1-128)

EVC Port DEI

Description:

Set or show port DEI mode.

Syntax:

EVC Port DEI [<port_list>] [<dei_mode>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<dei_mode> : DEI mode: coloured|fixed

EVC Port Tag

Description:

Set or show port tag match mode.

Syntax:

EVC Port Tag [<port_list>] [<tag_mode>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<tag_mode> : Tag mode: inner|outer

EVC Port Addr

Description:

Set or show port address match mode.

Syntax:

EVC Port Addr [<port_list>] [<addr_mode>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<addr_mode>: IP/MAC address mode: source|destination

EVC Port L2CP

Description:

Set or show port L2CP mode

Syntax:

EVC Port L2CP [<port_list>] [<l2cp_list>] [<mode>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<l2cp_list>: L2CP ID list (0-31). BPDU range: 0-15, GARP range: 16-31

<mode> : The mode takes the following values:

normal : Default forwarding

forward : Forward

redirect : Redirect to CPU

EVC Policer

Description:

Set or show EVC bandwidth profile.

Syntax:

EVC Policer [<policer_id>] [enable|disable] [<policer_mode>] [<cir>] [<cbs>] [<eir>] [<ebs>]

Parameters:

<policer_id> : Policer ID (1-128)

enable : Enable policer

disable : Disable policer

<policer_mode>: Policer_mode: coupled|aware

<cir> : Committed Information Rate [kbps]

<cbs> : Committed Burst Size [bytes]

<eir> : Excess Information Rate [kbps]

<ebs> : Excess Burst Size [bytes]

EVC Add

Description:

Add or modify EVC.

Syntax:

EVC Add <evc_id> [<vid>] [<ivid>] [<nni_list>] [<learning>] [inner] [<it_type>] [<it_vid_mode>] [<it_vid>] [<it_preserve>] [<it_pcp>] [<it_dei>] [outer] [<ot_vid>]

Parameters:

<evc_id> : EVC ID (1-128)

<vid> : EVC VLAN ID

<ivid> : Internal VLAN ID

<nni_list> : NNI port list (1-10) or 'none'

<learning> : Learning mode: enable|disable

inner : Inner tag action keyword

<it_type> : Inner tag type: none|c-tag|s-tag|s-custom-tag

<it_vid_mode>: Inner VID mode: normal|tunnel

<it_vid> : Inner tag VLAN ID (1-4095)

<it_preserve>: Inner tag preserved or fixed PCP/DEI: preserved|fixed

<it_pcp> : Inner tag PCP value (0-7)

<it_dei> : Inner tag DEI value (0-1)

outer : Outer tag action keyword

<ot_vid> : EVC outer tag VID for UNI ports

EVC Delete

Description:

Delete EVC.

Syntax:

EVC Delete <evc_id>

Parameters:

<evc_id>: EVC ID (1-128)

EVC Lookup

Description:

Lookup EVC.

Syntax:

EVC Lookup [<evc_id>]

Parameters:

<evc_id>: EVC ID (1-128)

EVC Status

Description:

Show EVC Status.

Syntax:

EVC Status [<evc_id>]

Parameters:

<evc_id>: EVC ID (1-128)

EVC Statistics

Description:

Show or clear EVC statistics.

Syntax:

EVC Statistics [<port_list>] [<class_list>] [<command>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<class_list>: QoS class list, 0-7

<command> : Statistics command: clear|green|yellow|red|discard

EVC ECE Add

Description:

Add or modify EVC Control Entry (ECE):

- If <ece_id> is specified and the ECE exists, the ECE will be modified.
- If <ece_id> is omitted or the ECE does not exist, a new ECE will be added.
- If <ece_id_next> is specified, the ECE will be placed before this entry.
- If <ece_id_next> is 'last', the ECE will be placed at the end of the list.
- If <ece_id_next> is omitted and it is a new ECE, the ECE will be placed last.
- If <ece_id_next> is omitted and the ECE exists, the ECE will not be moved.

Syntax:

EVC ECE Add [<ece_id>] [<ece_id_next>] [uni] [<uni_list>] [<dmac_type>] [<smac>][tag] [<tag_type>] [<vid>] [<pcp>] [<dei>] [all | (ipv4 [<proto>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<proto>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [direction] [<direction>] [evc] [<evc_id>] [pop] [<pop>] [policy] [<policy>] [class] [<class>] [outer] [<ot_mode>] [<ot_preserve>] [<ot_pcp>] [<ot_dei>]

Parameters:

<ece_id> : ECE ID (1-128)

<ece_id_next>: Next ECE ID (1-128) or 'last'

uni : UNI keyword

<uni_list> : UNI port list (1-10)

<dmac_type> : DMAC type: any|unicast|multicast|broadcast

<smac> : SMAC or 'any'

tag : Tag matching keyword

<tag_type> : Tag type: tagged|untagged|any

<vid> : VLAN ID value/range (0-4095) or 'any'

<pcp> : PCP value/range (0-7) or 'any'

<dei> : DEI value, 0, 1 or 'any'

all : Keyword for matching any frame type

ipv4 : Keyword for matching IPv4 frames

<proto> : IP protocol value (0-255) or 'any'

<sip> : IPv4 source address (a.b.c.d/n) or 'any'

<dscp> : DSCP value/range (0-63) or 'any'

<fragment> : IPv4 fragment: any|fragment|non-fragment

<sport> : UDP/TCP source port value/range (0-65535) or 'any'

<dport> : UDP/TCP destination port value/range (0-65535) or 'any'

ipv6 : Keyword for matching IPv6 frames

<sip_v6> : IPv6 source address (a.b.c.d/n) or 'any'

direction : Direction keyword

<direction> : ECE direction: both|uni-to-nni|nni-to-uni

evc : EVC keyword

<evc_id> : EVC ID (1-128) or 'none'

pop : Pop keyword

<pop> : Tag pop count: 0|1|2

policy : Policy keyword

<policy> : ACL policy number (0-255)

class : Class keyword

<class> : QoS class, 'disable' or 0-7

outer : Outer tag action keyword

<ot_mode> : Outer tag for nni-to-uni direction: enable|disable

<ot_preserve>: Outer tag preserved or fixed PCP/DEI: preserved|fixed

<ot_pcp> : Outer tag PCP value (0-7)

<ot_dei> : Outer tag DEI value (0-1)

EVC ECE Delete

Description:

Delete ECE.

Syntax:

EVC ECE Delete <ece_id>

Parameters:

<ece_id>: ECE ID (1-128)

EVC ECE Lookup

Description:

Lookup ECE.

Syntax:

EVC ECE Lookup [<ece_id>]

Parameters:

<ece_id>: ECE ID (1-128)

EVC ECE Status

Description:

Show ECE Status.

Syntax:

EVC ECE Status [<ece_id>]

Parameters:

<ece_id>: ECE ID (1-128)

6.17 Ethernet Protection Switching Command

EPS Create

Description:

EPS create.

Syntax:

EPS create [<inst>] [domport|dompath|domservice|dommpls] [1p1|1f1] [<flow_w>] [<flow_p>] [<mep_w>] [<mep_p>][<mep_aps>] [enable|disable]

Parameters:

<inst> : Instance number

domport|dompath|domservice|dommpls: Flow domain

1p1|1f1 : EPS architecture

<flow_w> : Working flow instance number

<flow_p> : Protecting flow instance number

<mep_w> : Working MEP instance number

<mep_p> : Protecting MEP instance number

<mep_aps> : APS MEP instance number

enable|disable : enable/disable protection

EPS Config

Description:

EPS config operation.

Syntax:

EPS config [<inst>] [aps|noaps] [revert|norevert] [unidir|bidir] [w0s|w10s|w30s|w1m|w5m|w12m][h0s|h100ms|h500ms|h1s|h2s|h5s|h10s]

Parameters:

<inst> : Instance number

aps|noaps : APS enable/disable

revert|norevert : Revertive enable/disable

unidir|bidir : Unidirectional or bidirectional switching

w0s|w10s|w30s|w1m|w5m|w12m : Wait to restore timer value

h0s|h100ms|h500ms|h1s|h2s|h5s|h10s: Hold off timer value

EPS Command

Description:

EPS command set operation.

Syntax:

EPS command [<inst>] [clear|lockout|forced|manualp|manualw|exercise|freeze|lockoutlocal]

Parameters:

<inst> : Instance number

clear|lockout|forced|manualp|manualw|exercise|freeze|lockoutlocal: EPS protection command type - clear is 'no command active'

EPS State

Description:

Get protection state.

Syntax:

EPS state [<inst>]

Parameters:

<inst>: Instance number

6.18 Maintainence entity End Point Command

MEP Config

Description:

MEP instance configuration

'mep|mip' this entity is either a MEP or a MIP - end point or intermediate point

'ingress|egress' this entity is either a Ingress (down) or Egress (up) type of MEP/MIP

'domport|domevc' the domain is either Port or EVC

'level' is the MEG level

'port' is the residence port

'flow' is the related flow instance number - Port number in Port domain - EVC number in EVC domain

'vid' is used for TAGGED OAM in port domain

'itu|ieee' is the MEG ID format

'meg' is the MEG ID - max. 8 char in case of 'ieee' - 6 or 7 char in case of 'itu'

'mep' is the MEP ID.

Syntax:

MEP config [<inst>] [mep|mip] [ingress|egress] [<port>] [domport|domevc] [<level>] [itu|ieee] [<meg>] [<mep>] [<vid>] [<flow>] [enable|disable]

Parameters:

<inst> : Instance number

mep|mip : Mode of the MEP instance

ingress|egress: Direction of the MEP instance

<port> : Port number.

domport|domevc: Flow domain

<level> : MEP level (0-7)

itu|ieee : MEG format

ITU: ICC format as defined in Y.1731 ANNEX A

IEEE: String format Domain Name and Short Name as defined in 802.1ag

<meg> : MEG ID (max. 8 chars)

<mep> : This MEP id (0-0x1FFF)

<vid> : C-TAG only applicable for Port MEP

<flow> : Flow instance number (Port/EVC)

enable|disable: enable/disable

MEP Peer MEP

Description:

MEP Peer MEP id configuration.

Syntax:

MEP peer MEP [<inst>] [<mep>] [<mac_addr>] [enable|disable]

Parameters:

<inst> : Instance number

<mep> : This MEP id (0-0x1FFF)

<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)

enable|disable: enable/disable

MEP Continuity Check Configuration

Description:

MEP Continuity Check configuration

'prio' is the priority (PCP) of transmitted CCM frame

'300s|100s|10s|1s|6m|1m|6h' is the number of CCM frame pr. second.

Syntax:

MEP cc config [<inst>] [<prio>] [300s|100s|10s|1s|6m|1m|6h] [enable|disable]

Parameters:

<inst> : Instance number

<prio> : OAM PDU priority

300s|100s|10s|1s|6m|1m|6h: OAM period (100s -> 100 PDU pr. second)

enable|disable : enable/disable

MEP Loss Measurement Configuration

Description:

MEP Loss Measurement configuration

'prio' is the priority (PCP) of transmitted LM frame

'uni|multi' is selecting uni-cast or multi-cast transmission of LM frame

'single|dual' is selecting single-ended (LMM) or dual-ended (CCM) LM

'10s|1s|6m|1m|6h' is the number of LM frame pr. second

'flr' is the Frame Loss Ratio time interval.

Syntax:

MEP lm config [<inst>] [<prio>] [uni|multi] [single|dual] [10s|1s|6m|1m|6h] [<flr>] [enable|disable]

Parameters:

<inst> : Instance number

<prio> : OAM PDU priority

uni|multi : Destination address is unicast or multicast

single|dual : LM is single or dual ended

10s|1s|6m|1m|6h: LM period (10s -> 10 PDU pr. second)

<flr> : Frame loss ratio (in sec.)

enable|disable : enable/disable

MEP APS Configuration

Description:

MEP APS configuration

'prio' is the priority (PCP) of transmitted APS frame

'uni|multi' is selecting uni-cast or multi-cast transmission of APS frame

'laps|raps' is selecting ELPS or ERPS protocol

'octet' is the last octet in RAPS multicast MAC.

Syntax:

MEP aps config [<inst>] [<prio>] [uni|multi] [laps|raps] [<octet>] [enable|disable]

Parameters:

<inst> : Instance number

<prio> : OAM PDU priority

uni|multi : Destination address is unicast or multicast

laps|raps : Selection of Linear or Ring APS type

<octet> : The last octet in RAPS multicast MAC

enable|disable: enable/disable

MEP Client Configuration

Description:

MEP Client configuration

'domport|domevc' is the client domain - must be EVC

'level' is the client MEG level - the contained level in the AIS and LCK frames

'cflow' is the client flow instance - up to 10 possible client flows (EVC).

Syntax:

MEP client config [<inst>] [domport|domevc] [<level>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>] [<cflow>]

Parameters:

<inst> : Instance number

domport|domevc: Flow domain

<level> : MEP level (0-7)

<cflow> : Client flow instance number (EVC)

MEP AIS Configuration

Description:

MEP AIS configuration

'prio' is the priority (PCP) of transmitted AIS frame

'1s|1m' is the number of AIS frame pr. second

'set|clear' is set or clear of protection usability. If set, the first 3 AIS frames are transmitted as fast as possible - this gives protection reliability in the path end-point.

Syntax:

MEP ais config [<inst>] [<prio>] [1s|1m] [set|clear] [enable|disable]

Parameters:

<inst> : Instance number

<prio> : OAM PDU priority

1s|1m : Transmit period for AIS

1s - to send OAM Frames in the rate of 1 per second

1m - to send OAM frames in the rate of 1 per minute

set|clear : Protection usability set/clear

enable|disable: enable/disable

MEP LCK Configuration

Description:

MEP LCK configuration

'prio' is the priority (PCP) of transmitted AIS frame

'1s|1m' is the number of AIS frame pr. second.

Syntax:

MEP lck config [<inst>] [<prio>] [1s|1m] [enable|disable]

Parameters:

<inst> : Instance number

<prio> : OAM PDU priority

1s|1m : Transmit period for LCK

1s - to send OAM Frames in the rate of 1 per second

1m - to send OAM frames in the rate of 1 per minute

enable|disable: enable/disable

MEP Link Trace Configuration

Description:

MEP Link Trace configuration

'prio' is the priority (PCP) of transmitted LTM frame

'mac_addr' is the unicast MAC of target MEP/MIP

'mep' is the peer MEP-ID of target MEP - only used if 'mac_addr is 'all zero'

'tll' is the TLL in the transmitted LTM.

Syntax:

MEP lt config [<inst>] [<prio>] [<mac_addr>] [<mep>] [<ttl>] [enable|disable]

Parameters:

<inst> : Instance number

<prio> : OAM PDU priority

<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)

<mep> : This MEP id (0-0x1FFF)

<ttl> : LT - Time To Live

enable|disable: enable/disable

MEP Loop Back Configuration

Description:

MEP Loop Back configuration

'set|clear' is set or clear of DEI of transmitted LBM frame

'prio' is the priority (PCP) of transmitted LBM frame

'uni|multi' is selecting uni-cast or multi-cast transmission of LBM frame

'mac_addr' is the unicast MAC of target MEP/MIP

'mep' is the peer MEP-ID of target MEP - only used if 'mac_addr is 'all zero'

'tosend' is the number of LBM to send

'size' is the size of the LBM data field

'gap' is the gap between LBM.

Syntax:

MEP lb config [<inst>] [set|clear] [<prio>] [uni|multi] [<mac_addr>] [<mep>] [<tosend>] [<size>] [<gap>] [enable|disable]

Parameters:

<inst> : Instance number

set|clear : OAM DEI set/clear

<prio> : OAM PDU priority

uni|multi : Destination address is unicast or multicast

<mac_addr> : MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)

<mep> : This MEP id (0-0x1FFF)

<tosend> : Number of LBM to send

<size> : Size of LBM data field in bytes (max 1400)

<gap> : Gap between LBM to send in 10ms. (max 100 - '0' is as fast as possible)

enable|disable: enable/disable

MEP Delay Measurement Configuration

Description:

MEP Delay Measurement configuration

'prio' is the priority (PCP) of transmitted DM frame

'uni|multi' is selecting uni-cast or multi-cast transmission of DM frame

'mep' is the peer MEP-ID of target MEP - only used if 'uni'

'oneway|twoway' is selecting one-way (1DM) or two-way (DMM) DM

'std|prop' is selecting standadized or proprietary DM. the latest is using off-standard follow-up message carrying the exact HW transmit timestamp

'rdtrp|flow' is selecting round-trip or flow delay calculation. Round-trip is not using the far-end timestamps to calculate the far-end residence time

'gap' Gap between transmitting 1DM/DMM PDU - in 10 ms.

'count' number of frames used for average calculation on the latest 'count' frames received

'us|ns' calculation results are shown in micro or nano seconds

'keep|reset' the action in case of total delay counter overflow - either 'keep' all results or 'reset' all results

'd2ford1' this is selecting to used two-way DMM for calculate one-way delay.

Syntax:

MEP dm config [<inst>] [<prio>] [uni|multi] [<mep>] [oneway|twoway] [std|prop] [rdtrp|flow] [<gap>] [<count>] [us|ns] [keep|reset] [d2ford1] [enable|disable]

Parameters:

<inst> : Instance number

<prio> : OAM PDU priority

uni|multi : Destination address is unicast or multicast

<mep> : This MEP id (0-0x1FFF)

oneway|twoway : DM is one-way or two-way

std|prop : Standard or Vitesse proprietary way(w/ follow-up packets) to send DM

rdtrp|flow : 2/4 timestamps selection

<gap> : Gap between 1DM/DMM to send in 10ms(10-65535).

<count> : The number of last records to calculate(10 - 2000)

us|ns : Time resolution

keep|reset : The action to counter when overflow happens

d2ford1 : Enable to use DMM/DMR packets to calculate one-way DM

enable|disable: enable/disable

MEP Test Signal Configuration

Description:

MEP Test Signal configuration

'set|clear' is set or clear of DEI of transmitted LBM frame

'prio' is the priority (PCP) of transmitted TST frame

'mep' is the peer MEP-ID of target MEP - only used if 'mac_addr is 'all zero'

'no_seq|seq' is without and with transmitted sequence numbers

'rate' is the TST frame transmission bit rate in Mbps'

'size' is the size of the un-tagged TST frame - four bytes will be added for each tag

'allzero|allone|onezero' is pattern contained in the TST frame data TLV.

Syntax:

MEP tst config [<inst>] [set|clear] [<prio>] [<mep>] [no_seq|seq] [<rate>] [<size>] [allzero|allone|onezero] [enable|disable]

Parameters:

<inst> : Instance number

set|clear : OAM DEI set/clear

<prio> : OAM PDU priority

<mep> : This MEP id (0-0x1FFF)

no_seq|seq : TST sequence number transmission

<rate> : Transmission bit rate of TST frames - in Mbps

<size> : Size of TST data field in bytes (max 1518)

allzero|allone|onezero: Data pattern to be filled in TST PDU

enable|disable : enable/disable

MEP State

Description:

MEP state get.

Syntax:

MEP state [<inst>]

Parameters:

<inst> : Instance number

MEP Loss Measurement State

Description:

MEP Loss Measurement state get.

Syntax:

MEP lm state [<inst>]

Parameters:

<inst> : Instance number

MEP Loss Measurement State Clear

Description:

MEP Loss Measurement state clear

Syntax:

MEP lm clear <inst>

Parameters:

<inst> : Instance number

MEP Link Trace State

Description:

MEP Link Trace state get.

Syntax:

MEP lt state [<inst>]

Parameters:

<inst> : Instance number

MEP Loop Back State

Description:

MEP Loop Back state get.

Syntax:

MEP lb state [<inst>]

Parameters:

<inst> : Instance number

MEP Delay Measurement State

Description:

MEP Delay Measurement state get.

Syntax:

MEP dm state [<inst>]

Parameters:

<inst> : Instance number

MEP Delay Measurement State Clear

Description:

MEP Delay Measurement state clear

Syntax:

MEP dm clear <inst>

Parameters:

<inst> : Instance number

MEP Test Signal State

Description:

MEP Test Signal state get

RX rate is shown in 100 Kbps.

Syntax:

MEP tst state [<inst>]

Parameters:

<inst> : Instance number

MEP Test Signal State Clear

Description:

MEP Test Signal state clear

Syntax:

MEP tst clear <inst>

Parameters:

<inst> : Instance number

6.19 Quality of Service Command

QoS Configuration

Description:

Show QoS Configuration.

Syntax:

QoS Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

QoS Port Classification Class

Description:

Set or show the default QoS class.

Syntax:

QoS Port Classification Class [<port_list>] [<class>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<class> : QoS class (0-7)

Default Setting:

0

Example:

Set default QoS class in 1 for port 1

```
NS3552-8P-2S:/>qos Port Classification Class 1 1
```

QoS Port Classification DPL

Description:

Set or show the default Drop Precedence Level.

Syntax:

QoS Port Classification DPL [<port_list>] [<dpl>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<dpl> : Drop Precedence Level (0-1)

Default Setting:

0

Example:

Set the default Drop Precedence Level in 1 for port1

```
NS3552-8P-2S:/>qos Port Classification dpl 1 1
```

QoS Port Classification PCP

Description:

Set or show the default PCP for an untagged frame.

Syntax:

QoS Port Classification PCP [<port_list>] [<pcp>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<pcp> : Priority Code Point (0-7)

Default Setting:

0

Example:

Set the default PCP for an untagged frame in 1 for port1

```
NS3552-8P-2S:/>qos Port Classification pcp 1 1
```

QoS Port Classification DEI

Description:

Set or show the default DEI for an untagged frame.

Syntax:

QoS Port Classification DEI [<port_list>] [<dei>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<dei> : Drop Eligible Indicator (0-1)

Default Setting:

0

Example:

Set the default DEI for an untagged frame in 1 for port1.

```
NS3552-8P-2S:/>qos Port Classification dei 1 1
```

QoS Port Classification Tag

Description:

Set or show if the classification is based on the PCP and DEI values in tagged frames.

Syntax:

QoS Port Classification Tag [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable tag classification

disable : Disable tag classification

(default: Show tag classification mode)

Default Setting:

disable

Example:

Enable QoS port classification Tag.

NS3552-8P-2S:/>**qos Port Classification tag 1-10 enable**

QoS Port Classification Map

Description:

Set or show the port classification map.

This map is used when port classification tag is enabled,and the purpose is to translate the Priority Code Point (PCP) and Drop Eligible Indicator (DEI) from a tagged frame to QoS class and DP level.

Syntax:

QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<pcp_list> : PCP list or 'all', default: All PCPs (0-7)

<dei_list> : DEI list or 'all', default: All DEIs (0-1)

<class> : QoS class (0-7)

<dpl> : Drop Precedence Level (0-1)

QoS Port Classification DSCP

Description:

Set or show if the classification is based on DSCP value in IP frames.

Syntax:

QoS Port Classification DSCP [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable DSCP based classification

disable : Disable DSCP based classification

(default: Show DSCP based classification mode)

Default Setting:

disable

Example:

Enable QoS port classification DSCP.

```
NS3552-8P-2S:/>qos Port Classification dscp 1-10 enable
```

QoS Port Policer Mode

Description:

Set or show the port policer mode

Syntax:

QoS Port Policer Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port policer

disable : Disable port policer

(default: Show port policer mode)

Default Setting:

disable

Example:

Enable QoS port policer

```
NS3552-8P-2S:/>qos Port Policer Mode 1-10 enable
```

QoS Port Policer Rate

Description:

Set or show the port policer rate.

Syntax:

QoS Port Policer Rate [<port_list>] [<rate>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<rate> : Rate in kbps or fps (100-15000000)

Default Setting:

500

Example:

Set the port policer rate in 1000

```
NS3552-8P-2S:/>qos Port Policer Rate 1-10 1000
```

QoS Port Policer Unit

Description:

Set or show the port policer unit.

Syntax:

QoS Port Policer Unit [<port_list>] [kbps|fps]

Parameters:

<port_list>: Port list or 'all', default: All ports

kbps : Unit is kilo bits per second

fps : Unit is frames per second

(default: Show port policer unit)

Default Setting:

kbps

Example:

Set the port policer unit in fps

```
NS3552-8P-2S:/>qos Port Policer unit 1-10 fps
```

QoS Port Policer Flow Control

Description:

Set or show the port policer flow control.

If policer flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Syntax:

QoS Port Policer FlowControl [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable port policer flow control

disable : Disable port policer flow control

(default: Show port policer flow control mode)

Default Setting:

disable

QoS Port QueuePolicer Mode

Description:

Set or show the port queue policer mode.

Syntax:

QoS Port QueuePolicer Mode [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list> : Port list or 'all', default: All ports

<queue_list>: Queue list or 'all', default: All queues (0-7)

enable : Enable port queue policer

disable : Disable port queue policer

(default: Show port queue policer mode)

Default Setting:

Disable

QoS Port QueuePolicer Rate

Description:

Set or show the port queue policer rate.

Syntax:

QoS Port QueuePolicer Rate [<port_list>] [<queue_list>] [<bit_rate>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<queue_list>: Queue list or 'all', default: All queues (0-7)

<bit_rate> : Rate in kilo bits per second (100-3300000)

Default Setting:

500

QoS Port Scheduler Mode

Description:

Set or show the port scheduler mode.

Syntax:

QoS Port Scheduler Mode [<port_list>] [strict|weighted]

Parameters:

<port_list>: Port list or 'all', default: All ports

strict : Strict mode

weighted: Weighted mode

(default: Show port scheduler mode)

Default Setting:

strict

Example:

Set the port schedule mode in weighted mode

```
NS3552-8P-2S:/>qos Port Scheduler Mode 1-10 weighted
```

QoS Port Scheduler Weight

Description:

Set or show the port scheduler weight.

Syntax:

QoS Port Scheduler Weight [<port_list>] [<queue_list>] [<weight>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<queue_list>: Weighted queue list or 'all', default: All weighted queues (0-5)

<weight> : Scheduler weight (1-100)

QoS Port QueueShaper Mode

Description:

Set or show the port queue shaper mode.

Syntax:

QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list> : Port list or 'all', default: All ports

<queue_list>: Queue list or 'all', default: All queues (0-7)

enable : Enable port queue shaper

disable : Disable port queue shaper

(default: Show port queue shaper mode)

Default Setting:

disable

Example:

Enable port queue shaper for all port & queue

```
NS3552-8P-2S:/>qos Port QueueShaper Mode 1-10 0-7 enable
```

QoS Port QueueShaper Rate

Description:

Set or show the port queue shaper rate.

Syntax:

QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<queue_list>: Queue list or 'all', default: All queues (0-7)

<bit_rate> : Rate in kilo bits per second (100-3300000)

Default Setting:

500kbps

Example:

Set the port queue shaper rate in 1000

```
NS3552-8P-2S:/>qos Port QueueShaper rate 1-10 0-7 1000
```

QoS Port QueueShaper Excess

Description:

Set or show the port queue excess bandwidth mode.

Syntax:

QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list> : Port list or 'all', default: All ports

<queue_list>: Queue list or 'all', default: All queues (0-7)

enable : Enable use of excess bandwidth

disable : Disable use of excess bandwidth

(default: Show port queue excess bandwidth mode)

Default Setting:

disable

Example:

Enable the port queue excess bandwidth mode.

```
NS3552-8P-2S:/>qos Port QueueShaper Excess 1-10 0-7 enable
```

QoS Port TagRemarking Mode

Description:

Set or show the port tag remarking mode.

Syntax:

QoS Port TagRemarking Mode [<port_list>] [classified|default|mapped]

Parameters:

<port_list>: Port list or 'all', default: All ports

classified: Use classified PCP/DEI values

default : Use default PCP/DEI values

mapped : Use mapped versions of QoS class and DP level

(default: Show port tag remarking mode)

Default Setting:

classified

Example:

Set the port tag remarking mode in mapped.

```
NS3552-8P-2S:/>qos Port TagRemarking Mode 1-10 mapped
```

QoS Port TagRemarking PCP

Description:

Set or show the default PCP. This value is used when port tag remarking mode is set to 'default'.

Syntax:

QoS Port TagRemarking PCP [<port_list>] [<pcp>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<pcp> : Priority Code Point (0-7)

Default Setting:

0

Example:

Set the default PCP in 1.

```
NS3552-8P-2S:/>qos Port TagRemarking PCP 1-10 1
```

QoS Port TagRemarking DEI

Description:

Set or show the default DEI. This value is used when port tag remarking mode is set to 'default'.

Syntax:

QoS Port TagRemarking DEI [<port_list>] [<dei>]

Parameters:

<port_list>: Port list or 'all', default: All ports

<dei> : Drop Eligible Indicator (0-1)

Default Setting:

0

Example:

Set the default EDI in 1.

```
NS3552-8P-2S:/>qos Port TagRemarking EDI 1-10 1
```

QoS Port TagRemarking Map

Description:

Set or show the port tag remarking map. This map is used when port tag remarking mode is set to 'mapped', and the purpose is to translate the classified QoS class (0-7) and DP level (0-1) to PCP and DEI.

Syntax:

QoS Port TagRemarking Map [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]

Parameters:

<port_list> : Port list or 'all', default: All ports

<class_list>: QoS class list or 'all', default: All QoS classes (0-7)

<dpl_list> : DP level list or 'all', default: All DP levels (0-1)

<pcp> : Priority Code Point (0-7)

<dei> : Drop Eligible Indicator (0-1)

QoS Port DSCP Translation

Description:

Set or show DSCP ingress translation mode.

If translation is enabled for a port, incoming frame DSCP value is translated and translated value is used for QoS classification.

Syntax:

QoS Port DSCP Translation [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable DSCP ingress translation

disable : Disable DSCP ingress translation

(default: Show DSCP ingress translation mode)

Default Setting:

disable

Example:

Enable DSCP ingress translation on all port.

```
NS3552-8P-2S:/>qos Port DSCP Translation 1-10 enable
```

QoS Port DSCP Classification

Description:

Set or show DSCP classification based on QoS class and DP level.

This enables per port to map new DSCP value based on QoS class and DP level.

Syntax:

QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]

Parameters:

<port_list>: Port list or 'all', default: All ports

none : No DSCP ingress classification

zero : Classify DSCP if DSCP = 0

selected : Classify DSCP for which class. mode is 'enable'

all : Classify all DSCP

(default: Show port DSCP ingress classification mode)

Default Setting:

none

Example:

Set DSCP classification based on QoS class and DP level in zero

```
NS3552-8P-2S:/> QoS Port DSCP Classification 1-10 zero
```

QoS Port DSCP EgressRemark

Description:

Set or show the port DSCP remarking mode.

Syntax:

QoS Port DSCP EgressRemark [<port_list>] [disable|enable|remap_dp_unaware|remap_dp_aware]

Parameters:

<port_list>: Port list or 'all', default: All ports

disable : Disable DSCP egress rewrite

enable : Enable DSCP egress rewrite with the value received from analyzer

remap_dp_unaware : Rewrite DSCP in egress frame with remapped DSCP where remap is DP unaware or DP = 0

remap_dp_aware : Rewrite DSCP in egress frame with remapped DSCP where remap is DP aware and DP = 1

(default: Show port DSCP egress remarking mode)

Default Setting:

disable

Example:

Enable DSCP egress rewrite

```
NS3552-8P-2S:/> QoS Port DSCP EgressRemark 1-10 enable
```

QoS DSCP Map

Description:

Set or show DSCP mapping table.

This table is used to map QoS class and DP level based on DSCP value.

DSCP value used to map QoS class and DPL is either translated DSCP value or incoming frame DSCP value.

Syntax:

QoS DSCP Map [<dscp_list>] [<class>] [<dpl>]

Parameters:

<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'

(default: Show DSCP ingress map table i.e. DSCP->(class, DPL))

<class> : QoS class (0-7)

<dpl> : Drop Precedence Level (0-1)

QoS DSCP Translation

Description:

Set or show global ingress DSCP translation table.

If port DSCP translation is enabled, translation table is used to translate incoming frames DSCP value and translated value is used to map QoS class and DP level.

Syntax:

QoS DSCP Translation [<dscp_list>] [<trans_dscp>]

Parameters:

<dscp_list> : DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'

(default: Show DSCP translation table)

<trans_dscp>: Translated DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43

QoS DSCP Trust

Description:

Set or show trusted DSCP value which is used for QoS classification.

The DSCP value to be checked for trust is either translated value ifDSCP translation is enabled for the ingress port or incoming frame DSCPvalue if translation is disabled for the port. Trusted DSCP value is onlyused for QoS classification.

Syntax:

QoS DSCP Trust [<dscp_list>] [enable|disable]

Parameters:

<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'

enable : Set DSCP as trusted DSCP

disable : Set DSCP as un-trusted DSCP

(default: Show DSCP Trust status)

Default Setting:

disable

QoS DSCP Classification Mode

Description:

Set or show DSCP ingress classification mode.

If port DSCP classification is 'selected', DSCP will be classified based on QoS class and DP level only for DSCP value with classification mode 'enabled'. DSCP may be translated DSCP if translation is enabled for the port.

Syntax:

QoS DSCP Classification Mode [<dscp_list>] [enable|disable]

Parameters:

<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'

enable : Enable DSCP ingress classification

disable : Disable DSCP ingress classification

(default: Show DSCP classification mode)

Default Setting:

disable

QoS DSCP EgressRemap

Description:

Set or show DSCP egress remap table. This table is used if the port egress remarking mode is 'remap' and the purpose is to map the DSCP and DP level to a new DSCP value.

Syntax:

QoS DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]

Parameters:

<dscp_list>: DSCP (0-63, BE, CS1-CS7, EF or AF11-AF43) list or 'all'

<dpl_list> : DP level list or 'all', default: All DP levels (0-1)

<dscp> : Egress remapped DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43

QoS Storm Unicast

Description:

Set or show the unicast storm rate limiter.

Syntax:

QoS Storm Unicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable unicast storm control

disable : Disable unicast storm control

<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k)

Default Setting:

disable

Example:

Enable unicast storm control in 2fps

```
NS3552-8P-2S:/> QoS Storm Unicast enable 2
```

QoS Storm Multicast

Description:

Set or show the multicast storm rate limiter.

Syntax:

QoS Storm Multicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable multicast storm control

disable : Disable multicast storm control

<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k)

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3552-8P-2S:/> QoS Storm multicast enable 2
```

QoS Storm Broadcast

Description:

Set or show the broadcast storm rate limiter. The limiter will only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Syntax:

QoS Storm Broadcast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable broadcast storm control

disable : Disable broadcast storm control

<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

Default Setting:

disable

QoS QCL Add

Description:

Add or modify QoS Control Entry (QCE).

If the QCE ID parameter <qce_id> is specified and an entry with this QCE ID already exists, the QCE will be modified. Otherwise, a new QCE will be added. If the QCE ID is not specified, the next available QCE ID will be used. If the next QCE ID parameter <qce_id_next> is specified, the QCE will be placed before this QCE in the list. If the next QCE ID is not specified and if it is a new entry added, the QCE will be placed last in the list. Otherwise if the next QCE ID is not specified and if existing QCE is modified, QCE will be in the same location in the list. To modify and move the entry to last in the list, use the word 'last' for <qce_id_next>.

Syntax:

QoS QCL Add [<qce_id>] [<qce_id_next>] [<port_list>] [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>] [(etype [<etype>]) | (LLC [<DSAP>] [<SSAP>] [<control>]) | (SNAP [<PID>]) | (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [<class>] [<dp>] [<classified_dscp>]

Parameters:

<qce_id> : QCE ID (1-256), default: Next available ID

<qce_id_next> : Next QCE ID: "next_id (1-256) or 'last'"

<port_list> : Port List: "port <port_list> or 'all'", default: All ports

<tag> : Frame tag: untag|tag|any

<vid> : VID: 1-4095 or 'any', either a specific VID or range of VIDs

<pcp> : Priority Code Point: specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'any'

<dei> : Drop Eligible Indicator: 0-1 or 'any'

<smac> : Source MAC address: (xx-xx-xx) or 'any', 24 MS bits (OUI)

<dmac_type> : Destination MAC type: unicast|multicast|broadcast|any

etype : Ethernet Type keyword

<etype> : Ethernet Type: 0x600-0xFFFF or 'any' but excluding 0x800(IPv4) and 0x86DD(IPv6)

llc : LLC keyword

<dsap> : Destination Service Access Point: 0x00-0xFF or 'any'

<ssap> : Source Service Access Point: 0x00-0xFF or 'any'

<control> : LLC control: 0x00-0xFF or 'any'

snap : SNAP keyword

<pid> : Protocol ID (EtherType) or 'any'

ipv4 : IPv4 keyowrd

<protocol> : IP protocol number: (0-255, TCP or UDP) or 'any'

<sip> : Source IP address: (a.b.c.d/n) or 'any'

<dscp> : DSCP:(0-63,BE,CS1-CS7,EF or AF11-AF43)or'any',specific/range

<fragment> : IPv4 frame fragmented: yes|no|any

<sport> : Source TCP/UDP port:(0-65535) or 'any',specific or port range

<dport> : Dest. TCP/UDP port:(0-65535) or 'any', specific or port range

ipv6 : IPv6 keyowrd

<sip_v6> : IPv6 source address: (a.b.c.d/n) or 'any', 32 LS bits

<class> : QoS Class: "class (0-7)", default: basic classification

<dp> : DP Level: "dp (0-1)", default: basic classification

<classified_dscp>: DSCP: "dscp (0-63, BE, CS1-CS7, EF or AF11-AF43)"

QoS QCL Delete

Description:

Delete QCE entry from QoS Control list.

Syntax:

QoS QCL Delete <qce_id>

Parameters:

<qce_id>: QCE ID (1-256), default: Next available ID

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3552-8P-2S:/> QoS Storm multicast enable 2
```

QoS QCL Lookup

Description:

Lookup QoS Control List.

Syntax:

QoS QCL Lookup [<qce_id>]

Parameters:

<qce_id>: QCE ID (1-256), default: Next available ID

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3552-8P-2S:/> QoS Storm multicast enable 2
```

QoS QCL Status

Description:

Show QCL status. This can be used to display if there is any conflict in QCE for differnet user types.

Syntax:

QoS QCL status [combined|static|voice_vlan|conflicts]

Parameters:

combined|static|voice_vlan|conflicts: combined **:** Shows the combined status

static : Shows the static user configured status

voice_vlan : Shows the status by Voice VLAN

conflicts : Shows all conflict status

(default : Shows the combined status)

QoS QCL Refresh

Description:

Resolve QCE conflict status. Same H/W resource is shared by multiple applications and it may not be available even before MAX QCE entry. So user can release the resource in use by other applications and use this command to acquire the resource.

Syntax:

QoS QCL refresh

Parameters:

combined|static|voice_vlan|conflicts: combined **:** Shows the combined status

static : Shows the static user configured status

voice_vlan : Shows the status by Voice VLAN

conflicts : Shows all conflict status

(default : Shows the combined status)

Default Setting:

disable

Example:

Enable multicast storm control in 2fps

```
NS3552-8P-2S:/> QoS Storm multicast enable 2
```

6.20 Mirror Command

Mirror Configuration

Description:

Show mirror configuration.

Syntax:

Mirror Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Example:

Show mirror configuration.

```
NS3552-8P-2S:/>mirror configuration
```

Mirror Port

Description:

Set or show the mirror port.

Syntax:

Mirror Port [<port>|disable]

Parameters:

<port>|disable: Mirror port or 'disable', default: Show port

Default Setting:

disable

Example:

Set port 2 for the mirror port.

```
NS3552-8P-2S:/>mirror port 2
```

Mirror Mode

Description:

Set or show the mirror mode.

Syntax:

Mirror Mode [<port_list>] [enable|disable|rx|tx]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Rx and Tx mirroring

disable: Disable Mirroring

rx : Enable Rx mirroring

tx : Enable Tx mirroring

(default: Show mirror mode)

Default Setting:

disable

Example:

Enable the mirror mode for port 1-4.

```
NS3552-8P-2S:/>mirror mode 1-4 enable
```

6.21 Configuration Command

Configuration Save

Description:

Save configuration to TFTP server.

Syntax:

Config Save <ip_server> <file_name>

Parameters:

<ip_server>: TFTP server IP address (a.b.c.d)

<file_name>: Configuration file name

Configuration Load

Description:

Load configuration from TFTP server.

Syntax:

Config Load <ip_server> <file_name> [check]

Parameters:

<ip_server>: TFTP server IP address (a.b.c.d)

<file_name>: Configuration file name

check : Check configuration file only, default: Check and apply file

6.22 Firmware Command

Firmware Load

Description:

Load new firmware from TFTP server.

Syntax:

Firmware Load <ip_addr_string> <file_name>

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

<file_name> : Firmware file name

Firmware IPv6 Load

Description:

Load new firmware from IPv6 TFTP server.

Syntax:

Firmware IPv6 Load <ipv6_server> <file_name>

Parameters:

<ipv6_server>: TFTP server IPv6 address

<file_name> : Firmware file name

Firmware Information

Description:

Display information about active and alternate firmware images.

Syntax:

Firmware Information

Firmware Swap

Description:

Activate the alternate firmware image..

Syntax:

Firmware Swap

6.23 UPnP Command

UPnP Configuration

Description:

Show UPnP configuration.

Syntax:

UPnP Configuration

Example:

Show UPnP configuration.

```
NS3552-8P-2S:/>upnp configuration

UPnP Configuration:
===================

UPnP Mode              : Disabled
UPnP TTL               : 4
UPnP Advertising Duration : 100
```

UPnP Mode

Description:

Set or show the UPnP mode.

Syntax:

UPnP Mode [enable|disable]

Parameters:

enable : Enable UPnP

disable: Disable UPnP

(default: Show UPnP mode)

Default Setting:

disable

Example:

Enable the UPnP mode.

```
NS3552-8P-2S:/>upnp mode enable
```

UPnP TTL

Description:

Set or show the TTL value of the IP header in SSDP messages.

Syntax:

UPnP TTL [<ttl>]

Parameters:

<ttl>: ttl range (1..255), default: Show UPnP TTL

Default Setting:

4

Example:

Set the value 10 for TTL value of the IP header in SSDP messages.

```
NS3552-8P-2S:/>upnp ttl 10
```

UPnP Advertising Duration

Description:

Set or show UPnP Advertising Duration.

Syntax:

UPnP Advertising Duration [<duration>]

Parameters:

<duration>: duration range (100..86400), default: Show UPnP duration range

Default Setting:

100

Example:

Set value 1000 for UPnP Advertising Duration.

```
NS3552-8P-2S:/>upnp advertising duration 1000
```

6.24 MVR Command

MVR Configuration

Description:

Show the MVR configuration.

Syntax:

MVR Configuration

Example:

Show the MVR configuration.

```
NS3552-8P-2S:/>mvr configuration

MVR Configuration:
==================

MVR Mode: Disabled
Muticast VLAN ID: 100

Port  Port Mode    Port Type    Immediate Leave
----  ----------  -----------  ---------------
1     Disabled    Receive      Disabled
2     Disabled    Receive      Disabled
3     Disabled    Receive      Disabled
4     Disabled    Receive      Disabled
5     Disabled    Receive      Disabled
6     Disabled    Receive      Disabled
7     Disabled    Receive      Disabled
8     Disabled    Receive      Disabled
9     Disabled    Receive      Disabled
10    Disabled    Receive      Disabled
```

MVR Mode

Description:

Set or show the MVR mode.

Syntax:

MVR Mode [enable|disable]

Parameters:

enable : Enable MVR mode

disable : Disable MVR mode

(default: Show MVR mode)

Default Setting:

disable

Example:

Enable MVR mode.

```
NS3552-8P-2S:/>mvr mode enable
```

MVR VLAN Setup

Description:

Set or show per MVR VLAN configuration.

Syntax:

MVR VLAN Setup [<mvid>] [add|del|upd] [(Name <mvr_name>)]

Parameters:

<mvid> : MVR VLAN ID (1-4095)

add : Add operation

del : Delete operation

upd : Update operation

name : MVR Name keyword

<mvr_name>: MVR VLAN name (Maximum of 32 characters)

MVR VLAN Mode

Description:

Set or show per MVR VLAN mode.

Syntax:

MVR VLAN Mode [<vid>|<mvr_name>] [dynamic|compatible]

Parameters:

<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)

dynamic : Dynamic MVR mode

compatible: Compatible MVR mode

(default: Show MVR VLAN mode)

MVR VLAN Port

Description:

Set or show per MVR VLAN port role.

Syntax:

MVR VLAN Port [<vid>|<mvr_name>] [<port_list>] [source|receiver|inactive]

Parameters:

<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)

<port_list> : Port list or 'all', default: All ports

source : MVR source port

receiver : MVR receiver port

inactive : Disable MVR

(default: Show MVR port role)

MVR VLAN LLQI

Description:

Set or show per MVR VLAN LLQI (Last Listener Query Interval).

Syntax:

MVR VLAN LLQI [<vid>|<mvr_name>] [mvr_param_llqi]

Parameters:

<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)

mvr_param_llqi :

-1 : Default Value (5)

0~31744 : Last Listener Query Interval in tenths of seconds

(default: Show MVR Interface Last Listener Query Interval

MVR VLAN Channel

Description:

Set or show per MVR VLAN channel.

Syntax:

MVR VLAN Channel [<vid>|<mvr_name>] [add|del|upd] [channel] [channel_bound] [(Name <grp_name>)]

Parameters:

<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)

add : Add operation

del : Delete operation

upd : Update operation

channel : IPv4/IPv6 multicast group address

channel_bound : The boundary IPv4/IPv6 multicast group address for the channel

name : MVR Name keyword

<grp_name> : MVR Channel name. (Maximum of 32 characters)

MVR VLAN Priority

Description:

Set or show per MVR VLAN priority and VLAN tag.

Syntax:

MVR VLAN Priority [<vid>|<mvr_name>] [priority] [tagged|untagged]

Parameters:

<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)

priority : CoS priority value ranges from 0 ~ 7

tagged : Tagged IGMP/MLD frames will be sent

untagged : Untagged IGMP/MLD frames will be sent

MVR Immediate Leave

Description:

Set or show MVR immediate leave per port.

Syntax:

MVR Immediate Leave [<port_list>] [enable|disable]

Parameters:

<<port_list>: Port list or 'all', default: All ports

enable : Enable Immediate Leave

disable : Disable Immediate Leave

(default: Show MVR Immediate Leave)

MVR Status

Description:

Show/Clear MVR operational status.

Syntax:

MVR Status [<vid>] [clear]

Parameters:

<vid>: VLAN ID (1-4095)

clear : Clear log

MVR Groups

Description:

Show MVR group addresses.

Syntax:

MVR Groups [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

MVR SFM

Description:

Show SFM (including SSM) related information for MVR.

Syntax:

MVR SFM [<vid>] [<port_list>]

Parameters:

<vid> : VLAN ID (1-4095)

<port_list>: Port list or 'all', default: All ports

6.25 Voice VLAN Command

Voice VLAN Configuration

Description:

Show Voice VLAN configuration.

Syntax:

Voice VLAN Configuration

Example:

Show Voice VLAN configuration.

```
NS3552-8P-2S:/>voice vlan configuration

V oice VLAN Configuration:
==========================

Voice VLAN Mode              : Disabled
Voice VLAN VLAN ID           : 1000
Voice VLAN Age Time(seconds)  : 86400
Voice VLAN Traffic Class      : 7

Voice VLAN OUI Table:
=====================

Telephony OUI Description
------------- -----------
00-03-6B      Cisco phones
00-0F-E2      H3C phones
00-60-B9      Philips and NEC AG phones
00-D0-1E      Pingtel phones
00-E0-75      Polycom phones
00-E0-BB      3Com phones
00-01-E3      Siemens AG phones

Voice VLAN Port Configuration:
==============================


Port  Mode      Security  Discovery Protocol
----  --------  --------  ------------------
1     Disabled  Disabled    OUI
2     Disabled  Disabled    OUI
3     Disabled  Disabled    OUI
4     Disabled  Disabled    OUI
5     Disabled  Disabled    OUI
6     Disabled  Disabled    OUI
7     Disabled  Disabled    OUI
8     Disabled  Disabled    OUI
9     Disabled  Disabled    OUI
10    Disabled  Disabled    OUI
```

Voice VLAN Mode

Description:

Set or show the Voice VLAN mode.

We must disable MSTP feature before we enable Voice VLAN.

It can avoid the conflict of ingress filter.

Syntax:

Voice VLAN Mode [enable|disable]

Parameters:

enable : Enable Voice VLAN mode.

disable: Disable Voice VLAN mode

(default: Show flow Voice VLAN mode)

Default Setting:

disable

Example:

Enable the Voice VLAN mode.

```
NS3552-8P-2S:/>voice vlan mode enable
```

Voice VLAN ID

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN ID [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

Default Setting:

1000

Example:

Set ID 2 for Voice VLAN ID.

```
NS3552-8P-2S:/>voice vlan id 2
```

Voice VLAN Agetime

Description:

Set or show Voice VLAN age time.

Syntax:

Voice VLAN Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (10-10000000) default: Show age time

Default Setting:

86400sec

Example:

Set Voice VLAN age time in 100sec.

```
NS3552-8P-2S:/>voice valn agetime 100
```

Voice VLAN Traffic Class

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN Traffic Class [<class>]

Parameters:

<class>: Traffic class (0-7)

Default Setting:

7

Example:

Set 4 traffic class for voice VLAN

```
NS3552-8P-2S:/>voice vlan traffic class4
```

Voice VLAN OUI Add

Description:

Add Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process. The maximum entry number is (16).

Syntax:

Voice VLAN OUI Add <oui_addr> [<description>]

Parameters:

<oui_addr> : OUI address (xx-xx-xx). The null OUI address isn't allowed

<description>: Entry description. Use 'clear' or "" to clear the string

No blank or space characters are permitted as part of a contact. (only in CLI)

Example:

Add Voice VLAN OUI entry.

```
NS3552-8P-2S:/>voice vlan oui add 00-11-22 test
```

Voice VLAN OUI Delete

Description:

Delete Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Delete <oui_addr>

Parameters:

<oui_addr>: OUI address (xx-xx-xx). The null OUI address isn't allowed

Example:

Delete Voice VLAN OUI entry.

```
NS3552-8P-2S:/>voice vlan oui delete 00-11-22
```

Voice VLAN OUI Clear

Description:

Clear Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Clear

Example:

Clear Voice VLAN OUI entry.

```
NS3552-8P-2S:/>voice vlan oui clear
```

Voice VLAN OUI Lookup

Description:

Clear Voice VLAN OUI entry. Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Clear

Example:

Lookup Voice VLAN OUI entry.

```
NS3552-8P-2S:/>voice vlan oui lookup
```

Voice VLAN Port Mode

Description:

Set or show the Voice VLAN port mode.

When the port mode isn't disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filter.

Syntax:

Voice VLAN Port Mode [<port_list>] [disable|auto|force]

Parameters:

<port_list>: Port list or 'all', default: All ports

disable : Disjoin from Voice VLAN.

auto : Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configure the Voice VLAN members automatically.

force : Forced join to Voice VLAN.

(default: Show Voice VLAN port mode)

Default Setting:

disable

Example:

Set auto mode for port 1-4 of Voice VLAN port mode.

```
NS3552-8P-2S:/>voice vlan port mode 1-4 auto
```

Voice VLAN Security

Description:

Set or show the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds.

Syntax:

Voice VLAN Security [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Voice VLAN security mode.

disable: Disable Voice VLAN security mode

(default: Show flow Voice VLAN security mode)

Default Setting:

disable

Example:

Enable the Voice VLAN port security mode for port 1-4.

```
NS3552-8P-2S:/>voice vlan security 1-4 enable
```

Voice VLAN Discovery Protocol

Description:

Set or show the Voice VLAN port discovery protocol mode. It only work under auto detect mode is enabled. We should enable LLDP feature before configure discovery protocol to 'LLDP' or 'Both'. Change discovery protocol to 'OUI' or 'LLDP' will restart auto detect process.

Syntax:

Voice VLAN Discovery Protocol [<port_list>] [oui|lldp|both]

Parameters:

<port_list>: Port list or 'all', default: All ports

OUI : Detect telephony device by OUI address.

LLDP : Detect telephony device by LLDP.

Both : Both OUI and LLDP.

(default: Show Voice VLAN discovery protocol)

Default Setting:

OUI

6.26 Ethernet Ring Protection Switching Command

ERPS Command

Description:

Invoking an administrative command for a given protection group

[fs|ms|clear] : setting or clearing an administrative command for a given group

<port> : forced a block on the ring port where this command is issued

<group_id> : protection group id

Syntax:

Erps command [fs|ms|clear] <port> <group-id>

Parameters:

fs|ms|clear: administrative commands

<port> : Port number

<group-id> : protection group id 1 - 64

ERPS Version

Description:

Specifying protocol version for a given protection group

[v1|v2] : specifying protocol version for a given protection group

<group_id> : protection group id

Syntax:

Erps version [v1|v2] <group-id>

Parameters:

v1|v2 : ERPS protocol version to be supported

<group-id>: protection group id 1 - 64

ERPS Add

Description:

create a new ethernet ring protection group

<group-id> : protection group id

<east_port> : protection group Port 0

<west_port> : protection group Port 1, Port 1 can be 0 for sub-rings

[major|sub] : ring type i.e major-ring or sub-ring

[interconnected] : interconnection node or not

[[virtual_channel] : Virtual channel present or not

[<major-ring-id>] : major ring group Id for interconnected sub-ring

Syntax:

Erps add <group-id> <east_port> <west_port> [major|sub] [interconnected] [virtual_channel] [<major-ring-id>]

Parameters:

<group-id> : protection group id 1 - 64

<east_port> : Port 0 of a protection group

<west_port> : Port 1 of a protection group

major|sub : ring type

interconnected : Set for interconnected node

virtual_channel: Set for virtual channel

<major-ring-id>: major ring of a sub-ring, when configuring as an interconnected node

ERPS Reversion

Description:

Configuring reversion characteristics for a given node

[revertive|nonrevertive] : enabling or disabling reversion for a given group

<group_id> : protection group id

Syntax:

Erps reversion [revertive|nonrevertive] <group-id>

Parameters:

revertive|nonrevertive: specifying reversion parameters

<group-id> : protection group id 1 - 64

ERPS VLAN Add

Description:

Associating a given vlan to a protection group

<vid> : vlan to be protected

<group-id> : protection group-id for which vid belongs to.

Syntax:

Erps vlan add <vid> <group-id>

Parameters:

<vid> : VLAN ID (1-4095)

<group-id>: protection group id 1 - 64

ERPS VLAN Delete

Description:

Disassociating a given vlan to a protection group

<vid> : protected vlan to be deleted

<group-id> : protection group-id for which vid belongs to.

Syntax:

Erps vlan delete <vid> <group-id>

Parameters:

<vid> : VLAN ID (1-4095)

<group-id>: protection group id 1 - 64

ERPS MEP

Description:

Associating Port 0/1 MEP to a protection group

<east_sf_mep> : Mep_ID for finding out Continuity Check errors on Port 0

<west_sf_mep> : Mep_ID for finding out Continuity Check errors on Port 1

<east_raps_mep> : Mep_ID for transmitting R-APS frames on Port 0

<west_raps_mep> : Mep_ID for transmitting R-APS frames on Port 1

<group_id> : protection group id for which mep is associating.

Syntax:

Erps mep <east_sf_mep> <west_sf_mep> <east_raps_mep> <west_raps_mep> <group-id>

Parameters:

<east_sf_mep> : SF mep id for Port 0

<west_sf_mep> : SF mep id for Port 1

<east_raps_mep>: CC/RAPS mep id for Port 0

<west_raps_mep>: CC/RAPS mep id for Port 1

<group-id> : protection group id 1 - 64

ERPS RPL Neighbour

Description:

Selection of RPL neighbour for a protection group

(east|west) : selected east(Port 0) or west(Port 1) as RPL neighbour

<group-id> : protection group id for selecting RPL Block.

Syntax:

Erps rpl neighbour <rpl_port> <group-id>

Parameters:

<rpl_port>: RPL Block

<group-id>: protection group id 1 - 64

ERPS RPL Owner

Description:

Selection of RPL Block for a protection group

by default this node is considered as RPL Owner

(east|west) : select east(Port 0) or west(Port 1) as RPL Block

<group-id> : protection group id for selecting RPL Block.

Syntax:

Erps rpl owner <rpl_port> <group-id>

Parameters:

<rpl_port>: RPL Block

<group-id>: protection group id 1 - 64

ERPS RPL Neighbour Clear

Description:

make this node as non-neighbour for a protection group

<group-id> : protection group id for selecting RPL Block.

Syntax:

Erps rpl neighbour clear <group-id>

Parameters:

<group-id>: protection group id 1 - 64

ERPS RPL Owner Clear

Description:

making a node as Non-RPL Block for a protection group

After clear, this node is nore an rpl owner for the given group

(east|west) : selected east(Port 0) or west(Port 1) as RPL Block

<group-id> : protection group id for selecting RPL Block.

Syntax:

Erps rpl owner clear <group-id>

Parameters:

<group-id>: protection group id 1 - 64

ERPS Hold Off Timeout

Description:

configuring hold off timeout for a protection group

in milliseconds 0-10000 in the increments of 100ms

<hold_timeout> : hold-off timeout

<group-id> : protection group id for configuring hold-off time.

Syntax:

Erps hold off timeout <hold_timeout> <group-id>

Parameters:

<hold_timeout>: timer timeout values

<group-id> : protection group id 1 - 64

ERPS Guard-timeout

Description:

configuring guard timeout for a protection group

guard timeout should be configured in the increments of 10 milliseconds

minimum guard timeout 10ms and maximum 2 seconds

<guard_timeout> : guard timeout

<group-id> : protection group id for configuring guard time.

Syntax:

Erps guard-timeout <guard_timeout> <group-id>

Parameters:

<guard_timeout>: timer timeout values

<group-id> : protection group id 1 - 64

ERPS WRT-timeout

Description:

configuring wait to restore timeout for a protection group

in minutes in the range of 1 to 12 minutes

<wtr_timeout> : configuring wtr timeout

<group-id> : protection group id for configuring wtr time.

Syntax:

Erps wtr-timeout <wtr_timeout> <group-id>

Parameters:

<wtr_timeout>: timer timeout values

<group-id> : protection group id 1 - 64

ERPS Delete

Description:

deletion of a protection group

<group-id> : protection group id for deletion .

Syntax:

Erps delete <group-id>

Parameters:

<group-id>: protection group id 1 - 64

ERPS Topologychange

Description:

specifying topology change propagation parameters for a given protection group

[propagate|nopropagate] : enabling or disabling topology change propagation for a given group

<group_id> : protection group id

.

Syntax:

Erps topologychange [propagate|nopropagate] <group-id>

Parameters:

propagate|nopropagate: topology change propagation configuration

<group-id> : protection group id 1 - 64

ERPS Configurationt

Description:

deletion of a protection group

<group-id> : protection group id

[statistics] : for displaying R-APS statistics

[clear] : for clearing R-APS statistics.

Syntax:

Erps configuration [<group-id>] [statistics|clear]

Parameters:

<group-id> : protection group id 1 - 64

statistics|clear: ERPS statistics

6.27 Loop Protect Command

Loop Protect Configuration

Description:

Show Loop Protection configuration.

Syntax:

Loop Protect Configuration

Loop Protect Mode

Description:

Set or show the Loop Protection mode.

Syntax:

Loop Protect Mode [enable|disable]

Parameters:

enable : Enable Loop Protection

disable: Disable Loop Protection

Default Setting:

enable

Loop Protect Transmit

Description:

Set or show the Loop Protection transmit interval.

Syntax:

Loop Protect Transmit [<transmit-time>]

Parameters:

Transmit time interval (1-10 seconds)

Default Setting:

5

Loop Protect Shutdown

Description:

Set or show the Loop Protection shutdown time.

Syntax:

Loop Protect Shutdown [<shutdown-time>]

Parameters:

Shutdown time interval (0-604800 seconds)

A value of zero disables re-enabling the port

Default Setting:

10

Loop Protect Port Configuration

Description:

Show Loop Protection port configuration.

Syntax:

Loop Protect Port Configuration [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

Loop Protect Port Mode

Description:

Set or show the Loop Protection port mode.

Syntax:

Loop Protect Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Loop Protection

disable: Disable Loop Protection

Loop Protect Port Action

Description:

Set or show the Loop Protection port action.

Syntax:

Loop Protect Port Action [<port_list>] [shutdown|shut_log|log]

Parameters:

<port_list>: Port list or 'all', default: All ports

shutdown : Shutdown the port

shut_log : Shutdown the port and Log event

log : (Only) Log the event

Loop Protect Port Transmit

Description:

Set or show the Loop Protection port transmit mode.

Syntax:

Loop Protect Port Transmit [<port_list>] [enable|disable]

Parameters:

<port_list>: Port list or 'all', default: All ports

enable : Enable Loop Protection

disable: Disable Loop Protection

Loop Protect Status

Description:

Show the Loop Protection status.

Syntax:

Loop Protect Status [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

6.28 IPMC Command

IPMC Configuration

Description:

Show IPMC snooping configuration.

Syntax:

IPMC Configuration [mld|igmp]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

IPMC Mode

Description:

Set or show the IPMC snooping mode.

Syntax:

IPMC Mode [mld|igmp] [enable|disable]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

enable : Enable IPMC snooping

disable: Disable IPMC snooping

(default: Show global IPMC snooping mode)

Default Setting:

disable

Example:

Enable IGMP snooping

```
NS3552-8P-2S:/>ipmc mode igmp enable
```

IPMC Flooding

Description:

Set or show the IPMC unregistered addresses flooding operation.

Syntax:

IPMC Flooding [mld|igmp] [enable|disable]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

enable : Enable IPMC flooding

disable: Disable IPMC flooding

(default: Show global IPMC flooding mode)

Default Setting:

enable

Example:

Enable IGMP flooding

```
NS3552-8P-2S:/>ipmc flooding igmp enable
```

IPMC Leave Proxy

Description:

Set or show the mode of IPMC Leave Proxy.

Syntax:

IPMC Leave Proxy [mld|igmp] [enable|disable]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

enable : Enable IPMC Leave Proxy

disable: Disable IPMC Leave Proxy

(default: Show global IPMC Leave Proxy mode)

Default Setting:

disable

Example:

Enable IGMP Leave Proxy

```
NS3552-8P-2S:/>ipmc leave proxy igmp enable
```

IPMC Proxy

Description:

Set or show the mode of IPMC Proxy.

Syntax:

IPMC Proxy [mld|igmp] [enable|disable]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

enable : Enable IPMC Proxy

disable: Disable IPMC Proxy

(default: Show global IPMC Proxy mode)

Default Setting:

disable

Example:

Enable IGMP Proxy

```
NS3552-8P-2S:/>ipmc proxy igmp enable
```

IPMC SSM

Description:

Set or show the IPMC SSM Range.

Syntax:

IPMC SSM [mld|igmp] [(Range <prefix> <mask_len>)]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

range : SSM Range keyword

<prefix> : IPv4/IPv6 multicast group address, accordingly

<mask_len>: Mask length for IPv4(4 ~ 32)/IPv6(8 ~ 128) ssm range, accordingly

IPMC VLAN Add

Description:

Add the IPMC snooping VLAN interface.

Syntax:

IPMC VLAN Add [mld|igmp] <vid>

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095)

IPMC VLAN Delete

Description:

Delete the IPMC snooping VLAN interface.

Syntax:

IPMC VLAN Delete [mld|igmp] <vid>

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095)

IPMC State

Description:

Set or show the IPMC snooping state for VLAN.

Syntax:

IPMC State [mld|igmp] [<vid>] [enable|disable]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

enable : Enable MLD snooping

disable: Disable MLD snooping

Default Setting:

disable

Example:

Enable IGMP snooping state for VLAN 1

```
NS3552-8P-2S:/>ipmc state igmp 1 enable
```

IPMC Querier

Description:

Set or show the IPMC snooping querier mode for VLAN.

Syntax:

IPMC Querier [mld|igmp] [<vid>] [enable|disable]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

enable : Enable MLD querier

disable: Disable MLD querier

Default Setting:

disable

Example:

Enable IGMP querier for VLAN 1

```
NS3552-8P-2S:/>ipmc querier igmp 1 enable
```

IPMC Compatibility

Description:

Set or show the IPMC Compatibility.

Syntax:

IPMC Compatibility [mld|igmp] [<vid>] [auto|v1|v2|v3]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

auto|v1|v2|v3:

auto : Auto Compatibility (Default Value)

v1 : Forced Compatibility of IGMPv1 or MLDv1

v2 : Forced Compatibility of IGMPv2 or MLDv2

v3 : Forced Compatibility of IGMPv3

(default: Show IPMC Interface Compatibility

IPMC Fastleave

Description:

Set or show the IPMC snooping fast leave port mode.

Syntax:

IPMC Fastleave [mld|igmp] [<port_list>] [enable|disable]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<port_list>: Port list or 'all', default: All ports

enable : Enable MLD fast leave

disable: Disable MLD fast leave

(default: Show IPMC fast leave mode)

Default Setting:

disable

Example:

Enable IGMP fast leave for all port

```
NS3552-8P-2S:/>ipmc fastleave igmp 1-10 enable
```

IPMC Throttling

Description:

Set or show the IPMC port throttling status.

Syntax:

IPMC Throttling [mld|igmp] [<port_list>] [limit_group_number]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<port_list>: Port list or 'all', default: All ports

0 : No limit

1~10 : Group learn limit

(default: Show IPMC Port Throttling)

Default Setting:

Unlimited

Example:

Set the max. learn 10 groups for ICMP port throttling

```
NS3552-8P-2S:/>ipmc throttling igmp 1-10 10
```

IPMC Filtering

Description:

Set or show the IPMC port group filtering list.

Syntax:

IPMC Filtering [mld|igmp] [<port_list>] [add|del] [group_addr]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<port_list>: Port list or 'all', default: All ports

add : Add new port group filtering entry

del : Del existing port group filtering entry

(default: Show IPMC port group filtering list)

group_addr : IPv4/IPv6 multicast group address, accordingly

IPMC Router

Description:

Set or show the IPMC snooping router port mode.

Syntax:

IPMC Router [mld|igmp] [<port_list>] [enable|disable]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<port_list>: Port list or 'all', default: All ports

enable : Enable IPMC router port

disable : Disable IPMC router port

(default: Show IPMC router port mode)

Example:

Enable port 1 in IPMC router port

```
NS3552-8P-2S:/>ipmc riuter igmp 1 enable
```

IPMC Status

Description:

Show IPMC operational status, accordingly.

Syntax:

IPMC Status [mld|igmp] [<vid>]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

Example:

Show VLAN 1 IPMC operational status

```
NS3552-8P-2S:/>ipmc status igmp 1
```

IPMC Group

Description:

Show IPMC group addresses, accordingly.

Syntax:

IPMC Groups [mld|igmp] [<vid>]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

Example:

Show VLAN 1 IPMC group addresses, accordingly.

```
NS3552-8P-2S:/>ipmc groups igmp 1
```

IPMC Version

Description:

Show IPMC Versions.

Syntax:

IPMC Version [mld|igmp] [<vid>]

Parameters:

mld|igmp:

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

Example:

Show VLAN 1 IPMC Versions.

```
NS3552-8P-2S:/>ipmc version igmp 1
```

IPMC SFM

Description:

Show SFM (including SSM) related information for IPMC.

Syntax:

IPMC SFM [mld|igmp] [<vid>] [<port_list>]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

<port_list>: Port list or 'all', default: All ports

IPMC Parameter RV

Description:

Set or show the IPMC Robustness Variable.

Syntax:

IPMC Parameter RV [mld|igmp] [<vid>] [ipmc_param_rv]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_rv:

-1 : Default Value (2)

1~255 : Robustness Variable

(default: Show IPMC Interface Robustness Variable

IPMC Parameter QI

Description:

Set or show the IPMC Query Interval.

Syntax:

IPMC Parameter QI [mld|igmp] [<vid>] [ipmc_param_qi]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_qi:

-1 : Default Value (125)

1~31744 : Query Interval in seconds

(default: Show IPMC Interface Query Interval

IPMC Parameter QRI

Description:

Set or show the IPMC Query Response Interval.

Syntax:

IPMC Parameter QRI [mld|igmp] [<vid>] [ipmc_param_qri]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_qri:

-1 : Default Value (100)

0~31744 : Query Response Interval in tenths of seconds

(default: Show IPMC Interface Query Response Interval

IPMC Parameter LLQI

Description:

Set or show the IPMC Last Listener Query Interval.

Syntax:

IPMC Parameter LLQI [mld|igmp] [<vid>] [ipmc_param_llqi]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_llqi:

-1 : Default Value (10)

0~31744 : Last Listener Query Interval in tenths of seconds

(default: Show IPMC Interface Last Listener Query Interval

IPMC Parameter URI

Description:

Set or show the IPMC Unsolicited Report Interval.

Syntax:

IPMC Parameter URI [mld|igmp] [<vid>] [ipmc_param_uri]

Parameters:

mld|igmp :

mld : IPMC for IPv6 MLD

igmp: IPMC for IPv4 IGMP

<vid> : VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_uri:

-1 : Default Value (1)

0~31744 : Unsolicited Report Interval in seconds

(default: Show IPMC Interface Unsolicited Report Interval)

6.29 VLAN Control List Command

VCL MAC-based VLAN Configuration

Description:

Show VCL MAC-based VLAN configuration.

Syntax:

VCL Macvlan Configuration

VCL MAC-based VLAN Add

Description:

Add or modify VCL MAC-based VLAN entry.

Syntax:

VCL Macvlan Add <mac_addr> <vid> [<port_list>]

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095)

<port_list>: Port list or 'all', default: All ports

Example:

Add 00-11-22-33-44-55-66 in VLAN 20 for all port

```
NS3552-8P-2S:/>vcl macvlan add 00-11-22-33-44-55-66 20 1-10
```

VCL MAC-based VLAN Delete

Description:

Delete VCL MAC-based VLAN entry.

Syntax:

VCL Macvlan Del <mac_addr>

Parameters:

<mac_addr> : MAC address (xx-xx-xx-xx-xx-xx)

Example:

Delete 00-11-22-33-44-55-66 in MAC-based VLAN list

```
NS3552-8P-2S:/> vcl macvlan del 00-11-22-33-44-55-66
```

VCL Stasus

Description:

Show VCL MAC-based VLAN users configuration.

Syntax:

VCL Status [combined|static|nas|all]

Parameters:

combined|static|nas|all: VCL User

VCL Protocol-based VLAN Add Ethernet II

Description:

Add VCL protocol-based VLAN Ethernet-II protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Add Eth2 <ether_type>|arp|ip|ipx|at <group_id>

Parameters:

<ether_type>|arp|ip|ipx|at: Ether Type (0x0600 - 0xFFFF)

<group_id> : Protocol group ID

VCL Protocol-based VLAN Add SNAP

Description:

Add VCL protocol-based VLAN SNAP protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Add Snap <oui>|rfc_1042|snap_8021h <pid> <group_id>

Parameters:

<oui>|rfc_1042|snap_8021h: OUI value (Hexadecimal 00-00-00 to FF-FF-FF).

<pid> : PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600-0xFFFF.

<group_id> : Protocol group ID

VCL Protocol-based VLAN Add LLC

Description:

Add VCL protocol-based VLAN LLC protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Add Llc <dsap> <ssap> <group_id>

Parameters:

<dsap> : DSAP value (0x00-0xFF)

<ssap> : SSAP value (0x00-0xFF)

<group_id>: Protocol group ID

VCL Protocol-based VLAN Delete Ethernet II

Description:

Delete VCL protocol-based VLAN Ethernet-II protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Delete Eth2 <ether_type>|arp|ip|ipx|at

Parameters:

<ether_type>|arp|ip|ipx|at: Ether Type (0x0600 - 0xFFFF)

VCL Protocol-based VLAN Delete SNAP

Description:

Delete VCL protocol-based VLAN SNAP protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Delete Snap <oui>|rfc_1042|snap_8021h <pid>

Parameters:

<oui>|rfc_1042|snap_8021h: OUI value (Hexadecimal 00-00-00 to FF-FF-FF).

<pid> : PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600-0xFFFF.

VCL Protocol-based VLAN Delete LLC

Description:

Delete VCL protocol-based VLAN LLC protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Delete Llc <dsap> <ssap>

Parameters:

<dsap>: DSAP value (0x00-0xFF)

<ssap>: SSAP value (0x00-0xFF)

VCL Protocol-based VLAN Add

Description:

Add VCL protocol-based VLAN group to VLAN mapping.

Syntax:

VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid>

Parameters:

<port_list>: Port list or 'all', default: All ports

<group_id> : Protocol group ID

<vid> : VLAN ID (1-4095)

VCL Protocol-based VLAN Delete

Description:

Delete VCL protocol-based VLAN group to VLAN mapping.

Syntax:

VCL ProtoVlan Vlan Delete [<port_list>] <group_id>

Parameters:

<port_list>: Port list or 'all', default: All ports

<group_id> : Protocol group ID

VCL Protocol-based VLAN Configuration

Description:

Show VCL protocol-based VLAN entries.

Syntax:

VCL ProtoVlan Conf

VCL IP Subnet-based Vlan Configuration

Description:

Show VCL IP Subnet-based VLAN configuration.

Syntax:

VCL IPVlan Configuration [<vce_id>]

Parameters:

<vce_id>: Unique VCE ID (1-128) for each VCL entry

VCL IP Subnet-based Vlan Add

Description:

Add or modify VCL IP Subnet-based VLAN entry. The maximum IPVlan entries are limited to 128.

Syntax:

VCL IPVlan Add [<vce_id>] <ip_addr_mask> <vid> [<port_list>]

Parameters:

<vce_id> : Unique VCE ID (1-128) for each VCL entry

<ip_addr_mask>: Source IP address and mask (Format: a.b.c.d/n).

<vid> : VLAN ID (1-4095)

<port_list> : Port list or 'all', default: All ports

VCL IP Subnet-based Vlan Delete

Description:

Delete VCL IP Subnet-based VLAN entry.

Syntax:

VCL IPVlan Delete <vce_id>

Parameters:

<vce_id>: Unique VCE ID (1-128) for each VCL entry

6.30 SMTP Command

SMTP Configuration

Description:

Show SMTP configure.

Syntax:

SMTP Configuration

Default Setting:

disable

SMTP Mode

Description:

Enable or disable SMTP configure.

Syntax:

SMTP Mode [enable|disable]

Parameters:

enable : Enable SMTP mode

disable : Disable SMTP mode

(default: Show SMTP mode)

Default Setting:

Disable

SMTP Server

Description:

Set or show SMTP server configure.

Syntax:

SMTP Server [<server>] [<port>]

Parameters:

<server>: SMTP server address

<port> : SMTP server port

Default Setting:

disable

SMTP Auth

Description:

Enable or disable SMTP authentication configure.

Syntax:

SMTP Auth [enable|disable]

Parameters:

enable : Enable SMTP Authentication

disable : Disable SMTP Authentication

(default: Show SMTP Authentication)

Default Setting:

disable

SMTP Auth_user

Description:

Set or show SMTP authentication user name configure.

Syntax:

SMTP Auth_user [<auth_user_text>]

Parameters:

<auth_user_text>: SMTP Authentication User Name

Default Setting:

disable

SMTP Auth_pass

Description:

Set or to show SMTP authentication password configure.

Syntax:

SMTP Auth_pass [<auth_pass_text>]

Parameters:

<auth_pass_text>: SMTP Authentication Password

Default Setting:

disable

SMTP Mail from

Description:

Set or show SMTP e-mail from configure.

Syntax:

SMTP Mailfrom [<mailfrom_text>]

Parameters:

<mailfrom_text>: SMTP E-mail From address

Default Setting:

Disable

SMTP Mail Subject

Description:

Set or to show SMTP e-mail subject configure.

Syntax:

SMTP Mailsubject [<mailsubject_text>]

Parameters:

<mailsubject_text>: SMTP E-mail Subject

Default Setting:

Disable

SMTP Mail to 1

Description:

Set or show SMTP e-mail 1 to configure.

Syntax:

SMTP Mailto1 [<mailto1_text>]

Parameters:

<mailto1_text>: SMTP e-mail 1 to address

Default Setting:

Disable

SMTP Mail to 2

Description:

Set or show SMTP e-mail 2 to configure.

Syntax:

SMTP Mailto2 [<mailto2_text>]

Parameters:

<mailto1_text>: SMTP e-mail 2 to address

Default Setting:

Disable

SMTP Test

Description:

Test the status for linking to SMTP server

Syntax:

SMTP Test

6.31 DIDO Command

DIDO DI Act

Description:

Set or show the system digital input0/1 action.

Syntax:

DIDO Di_act [first|second] [1|2] [enable|disable]

Parameters:

first : Digital Input/Output 0

second : Digital Input/Output 1

(default: Set or show digital input/output first(0)/second(1) select)

1 : System Log

2 : SNMP Trap

(default: set or show digital input 0/1 action)

enable : Enable digital input0/1 function

disable : Disable digital input0/1 function

(default: Set or show digital input/output/fault alarm 0/1 status)

DIDO DI Desciption

Description:

Set or show the system digital input0/1 description.

Syntax:

DIDO Di_desc [first|second] [<description>]

Parameters:

first : Digital Input/Output 0

second : Digital Input/Output 1

(default: Set or show digital input/output first(0)/second(1) select)

<description>: Digital input0/1 described string. Use 'clear' or "" to clear the string In CLI, no blank or space characters are permitted as part of a contact.

DIDO DI Enable

Description:

Set or show the system digital input0/1.

Syntax:

DIDO Di_en [first|second] [enable|disable] [hightolow|lowtohigh]

Parameters:

first : Digital Input/Output 0

second : Digital Input/Output 1

(default: Set or show digital input/output first(0)/second(1) select)

enable : Enable digital input0/1 function

disable : Disable digital input0/1 function

(default: Set or show digital input/output/fault alarm 0/1 status)

hightolow : Trigger -> high to low

lowtohigh : Trigger -> low to high

(default: Set or show digital input/output 0/1 trigger)

DIDO DO Act

Description:

Set or show the system digital output0/1 action.

Syntax:

DIDO Do_act [first|second] [port|power] [enable|disable]

Parameters:

first : Digital Input/Output 0

second : Digital Input/Output 1

(default: Set or show digital input/output first(0)/second(1) select)

port : port fail

power : power fail

DI1 : DI1 trigger

DI2 : DI2 trigger

(default: Set or show digital output/fault alarm 0/1 action)

enable : Enable digital input0/1 function

disable : Disable digital input0/1 function

(default: Set or show digital input/output/fault alarm 0/1 status)

DIDO DO Enable

Description:

Set or show the system digital output0/1.

Syntax:

DIDO Do_en [first|second] [enable|disable] [hightolow|lowtohigh]

Parameters:

first : Digital Input/Output 0

second : Digital Input/Output 1

(default: Set or show digital input/output first(0)/second(1) select)

enable : Enable digital input0/1 function

disable : Disable digital input0/1 function

(default: Set or show digital input/output/fault alarm 0/1 status)

hightolow : Trigger -> high to low

lowtohigh : Trigger -> low to high

(default: Set or show digital input/output 0/1 trigger)

DIDO DO Port Alarm

Description:

Set or show the system digital output0/1 port alarm.

Syntax:

DIDO Do_port_alr [first|second] [<port_list>]

Parameters:

first : Digital Input/Output 0

second : Digital Input/Output 1

(default: Set or show digital input/output first(0)/second(1) select)

<port_list>: Port list or 'all', default: All ports

DIDO DO Power Alarm

Description:

Set or show the system digital output0/1 power alarm.

Syntax:

DIDO Do_pwr_alr [first|second] [dc1|dc2] [enable|disable]

Parameters:

first : Digital Input/Output 0

second : Digital Input/Output 1

(default: Set or show digital input/output first(0)/second(1) select)

dc1 : DC power 1

dc2 **:** DC power 2

(default: Set or show digital output/fault alarm 0/1 power_fail)

enable : Enable digital input0/1 function

disable : Disable digital input0/1 function

(default: Set or show digital input/output/fault alarm 0/1 status)

DIDO Fault Act

Description:

Set or show the system fault alarm action.

Syntax:

DIDO Fault_act [port|power] [enable|disable]

Parameters:

port : port fail

power : power fail

DI1 : DI1 trigger

DI2 : DI2 trigger

(default: Set or show digital output/fault alarm 0/1 action)

enable : Enable digital input0/1 function

disable : Disable digital input0/1 function

(default: Set or show digital input/output/fault alarm 0/1 status)

DIDO Fault Enable

Description:

Set or show the system fault alarm.

Syntax:

DIDO Fault_en [enable|disable]

Parameters:

enable : Enable digital input0/1 function

disable : Disable digital input0/1 function

(default: Set or show digital input/output/fault alarm 0/1 status)

DIDO Fault Port Alarm

Description:

Set or show the system fault alarm of port alarm.

Syntax:

DIDO Fault_port_alr [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

DIDO Fault Power Alarm

Description:

Set or show the system fault alarm of power alarm.

Syntax:

DIDO Fault_pwr_alr [dc1|dc2] [enable|disable]

Parameters:

dc1 : DC power 1

dc2 : DC power 2

(default: Set or show digital output/fault alarm 0/1 power_fail)

enable : Enable digital input0/1 function

disable : Disable digital input0/1 function

(default: Set or show digital input/output/fault alarm 0/1 status)

6.32 Show Command

Show Access

Description:

Show access management configuration.

Syntax:

Show access

Show ACL

Description:

Show ACL Configuration.

Syntax:

Show acl

Show Aggregation

Description:

Show link aggregation configuration.

Syntax:

Show aggr

Show ARP

Description:

Show ARP inspection configuration.

Syntax:

Show arp

Show Auth

Description:

Show Auth configuration.

Syntax:

Show auth

Show DHCP Relay

Description:

Show DHCP relay configuration.

Syntax:

Show DHCP relay

Show EEE

Description:

Show EEE configuration.

Syntax:

Show EEE

Show HTTPs

Description:

Show HTTPS configuration.

Syntax:

Show https

Show IGMP

Description:

Show IPMC snooping configuration.

Syntax:

Show igmp

Show IP

Description:

Show IP configuration.

Syntax:

Show ip

Show LACP

Description:

Show LACP configuration.

Syntax:

Show lacp

Show Limit Control

Description:

Show Limit Control configuration.

Syntax:

Show limit control

Show LLDP

Description:

Show LLDP configuration.

Syntax:

Show lldp

Show LLDP-MED

Description:

Show LLDP-MED configuration.

Syntax:

Show LLDPMED

Show Loop Protect

Description:

Show Loop Protection configuration.

Syntax:

Show Loop Protect

Show MAC

Description:

Show MAC address table configuration.

Syntax:

Show MAC

Show Mirror

Description:

Show mirror configuration.

Syntax:

Show mirror

Show MVR

Description:

Show MVR configuration.

Syntax:

Show MVR

Show PoE

Description:

Show PoE configuration.

Syntax:

Show PoE

Show Port

Description:

Show port configuration.

Syntax:

Show port

Show Privilege

Description:

Show privilege configuration.

Syntax:

Show privilege

Show Private VLAN

Description:

Show Private VLAN configuration.

Syntax:

Show pvlan

Show QoS

Description:

Show QoS Configuration.

Syntax:

Show QoS

Show SNMP

Description:

Show SNMP configuration.

Syntax:

Show SNMP

Show SSH

Description:

Show SSH configuration.

Syntax:

Show ssh

Show System

Description:

Show system configuration.

Syntax:

Show system

Show Timezone

Description:

Show System Timezone configuration.

Syntax:

Show timezone

Show UPnP

Description:

Show UPnP configuration.

Syntax:

Show upnp

Show Users

Description:

Show users configuration.

Syntax:

Show users

Show VLAN

Description:

Show VLAN configuration.

Syntax:

Show vlan

Show Voice VLAN

Description:

Show Voice VLAN configuration.

Syntax:

Show voice vlan

Show Firmware

Description:

Display information about active and alternate firmware images.

Syntax:

Show firmware

Show STP

Description:

Show STP Port configuration.

Syntax:

Show STP

7. SWITCH OPERATION

7.1 Address Table

The **Industrial Managed Switch** is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This in-formation comes from the learning process of **Industrial Managed Switch**.

7.2 Learning

When one packet comes in from any port, the **Industrial Managed Switch** will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

7.3 Forwarding & Filtering

When one packet comes from some port of the **Industrial Managed Switch**, it will also check the destination address besides the source address learning. The **Industrial Managed Switch** will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the **Industrial Managed Switch** will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

7.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward **Industrial Managed Switch** stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The **Industrial Managed Switch** scans the destination address from the packet-header, searches the routing table pro-vided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. How-ever, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to signifi-cantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the **Industrial Managed Switch**, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The **Industrial Managed Switch** performs **"Store and Fforward"** therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

7.5 Auto-Negotiation

The STP ports on the **Industrial Managed Switch** have built-in **"Auto-negotiation"**. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode. 1000Base-T can be only connected in Full-duplex mode.

8. TROUBLE SHOOTING

This chapter contains information to help you solve problems. If the **Industrial Managed Switch** is not functioning properly, make sure the Ethernet Switch was set up according to instructions in this manual.

The per port LED is not lit

Solution:

Check the cable connection of the **Industrial Managed Switch**.

Performance is bad

Solution:

Check the speed duplex mode of the partner device. The **Industrial Managed Switch** is run at Auto-negotiation mode and if the partner is set to half duplex, then the performance will be poor.

Per port LED is lit, but the traffic is irregular

Solution:

Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

Why the Industrial Managed Switch doesn't connect to the network

Solution:

Check per port LED on the **Industrial Managed Switch**. Try another port on the **Industrial Managed Switch** Make sure the cable is installed properly Make sure the cable is the right type Turn off the power. After a while, turn on power again.

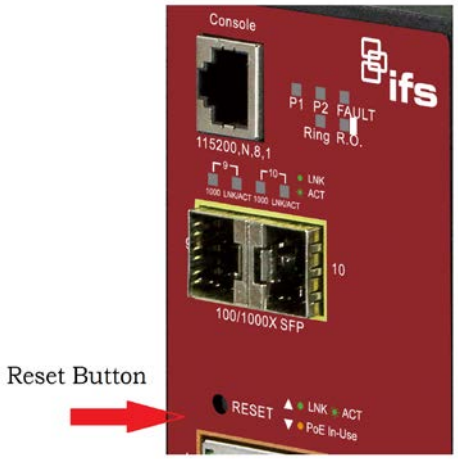
Can I install MGB-SX or other non wide temperature SFP module into SFP slot of Industrial Managed Switch?

Solution:

Yes, it does. However, since the MGB-SX and other non wide temperature SFP module cannot operate under -40 to 75 Degree C. Please pay attention to this point and consider use IFS wide temperature SFP module for **Industrial Managed Switch**.

■ **While IP Address be changed or forgotten admin password** –

To reset the IP address to the default IP Address **"192.168.0.100"** or reset the password to default value. Press the hardware **reset button** at the front panel about **10 seconds.** After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



APPENDEX A

A.1 Switch's Data RJ-45 Pin Assignments - 1000Mbps, 1000Base-T

PIN NO	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

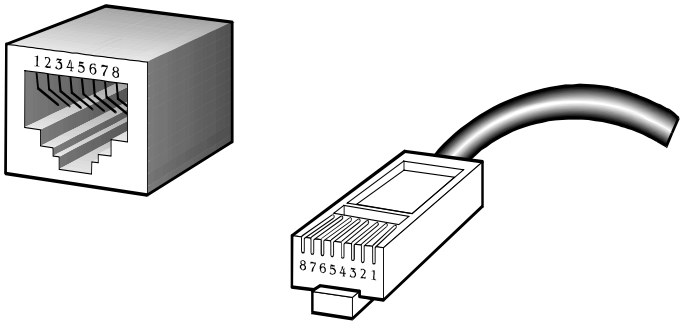
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	**MDI** **Media Dependant Interface**	**MDI-X** **Media Dependant Interface-Cross**
1	**Tx + (transmit)**	**Rx + (receive)**
2	**Tx - (transmit)**	**Rx - (receive)**
3	**Rx + (receive)**	**Tx + (transmit)**
4, 5	**Not used**	
6	**Rx - (receive)**	**Tx - (transmit)**
7, 8	**Not used**	

The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

		SIDE 1	SIDE2
Straight Cable			
1 2 3 4 5 6 7 8	SIDE 1	1 = White / Orange	1 = White / Orange
		2 = Orange	2 = Orange
		3 = White / Green	3 = White / Green
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Green
		7 = White / Brown	7 = White / Brown
		8 = Brown	8 = Brown
1 2 3 4 5 6 7 8	SIDE 2		
Crossover Cable		SIDE 1	SIDE2
1 2 3 4 5 6 7 8	SIDE 1	1 = White / Orange	1 = White / Green
		2 = Orange	2 = Green
		3 = White / Green	3 = White / Orange
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Orange
		7 = White / Brown	7 = White / Brown
		8 = Brown	8 = Brown
1 2 3 4 5 6 7 8	SIDE 2		

Figure A-1: Straight-Through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.

APPENDEX B: GLOSSARY

A

ACE

ACE is an acronym for **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

`ACL|Access Control List`: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.
`ACL|Ports`: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.
`ACL|Rate Limiters`: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate

Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for **A**uto **M**edia **S**elect. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the prefered media.

APS

APS is an acronym for **A**utomatic **P**rotection **S**witching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel is to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port Aggregation*, *Link Aggregation*).

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for **C**ontinuity **C**heck. It is a MEP functionality that is able to detect loss of continuity in a network by

transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for **C**ontinuity **C**heck **M**essage. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for **D**enial of **S**ervice. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.
An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 corresponds to 'Discard Eligible' (Yellow) frames.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP** **M**ulti**C**ast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 **L**ogical **L**ink **C**ontrol (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **L**ink **L**ayer **D**iscovery **P**rotocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximun response time used to calculate the Maximun Respse Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if there’s no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for **M**aintenance **E**ntity **E**ndpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for **M**essage-**D**igest algorithm **5**. MD5 is a message digest algorithm, used cryptographic hash

function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the **M**ultiple **S**panning **T**ree **P**rotocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them(Wikipedia).

N

NAS

NAS is an acronym for **N**etwork **A**ccess **S**erver. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for **Net**work **B**asic **I**nput/**O**utput **S**ystem. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for **N**etwork **F**ile **S**ystem. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for **P**riority **C**ode **P**oint. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for **P**owered **D**evice. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implements the Ethernet physical layer (IEEE-802.3).

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the

packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for **P**ower **O**ver **E**thernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for **P**ost **O**ffice **P**rotocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet.

It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports

configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a

given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SHA

SHA is an acronym for **S**ecure **H**ash **A**lgorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The **S**ub**N**etwork **A**ccess **P**rotocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack **P**rotocol using **ROU**ting **T**echnology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service **S**et **I**dentifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to base on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for **S**ecure **SH**ell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**cess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **TEL**etype **NET**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for **T**emporal **K**ey **I**ntegrity **P**rotocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

It is Virtual LAN. It is a method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

WEP is an acronym for **W**ired **E**quivalent **P**rivacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages is using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

WiFi is an acronym for **Wi**reless **Fi**delity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for **W**i-Fi **P**rotected **A**ccess. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for **W**i-Fi **P**rotected **A**ccess - **P**re **S**hared **K**ey. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for **W**i-Fi **P**rotected **A**ccess - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for **W**i-Fi **P**rotected **S**etup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for **W**eighted **R**andom **E**arly **D**etection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for **W**ait **T**o **R**estore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is.